Attorney Docket No. 1506.1041

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Atsuji SEKIGUCHI

Application No.: Unassigned | Group Art Unit: Unassigned

Filed: February 25, 2004 | Examiner: Unassigned

For: ROUTING LOOP DETECTION PROGRAM AND ROUTING LOOP DETECTION METHOD

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-326173

Filed: September 18, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 25, 2004 By: David M. Pitcher

David M. Pitcher
Registration No. 25,908

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　９月１８日

出願番号
Application Number: 特願２００３－３２６１７３

[ST. 10/C]: ［ＪＰ２００３－３２６１７３］

出願人
Applicant(s): 富士通株式会社

２００３年１２月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３１０５３４７

【書類名】　特許願
【整理番号】　0351732
【提出日】　平成15年 9月18日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 13/00
H04L 12/28
H04L 12/56
H04L 29/14
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　関口　敦二
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100098235
【弁理士】
【氏名又は名称】　金井　英幸
【電話番号】　03-5283-3188
【手数料の表示】
【予納台帳番号】　062606
【納付金額】　21,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9908696

【書類名】特許請求の範囲
【請求項１】
コンピュータを、
ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出手段，
前記パケット抽出手段が抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先ＩＰアドレスを読み取る読取手段，
前記読取手段が読み取った送信先ＩＰアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信手段，
前記パケット送信手段が送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信手段，及び、
前記パケット受信手段が受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティングループが発生している旨を出力する出力手段
として機能させる
ことを特徴とするルーティングループ検出プログラム。
【請求項２】
前記調査用パケットは、アプリケーション層上に存在するネットワークアプリケーションサービスについてのサービス要求パケットである
ことを特徴とする請求項１記載のルーティングループ検出プログラム。
【請求項３】
コンピュータを、
ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をＩＰヘッダ中に有するパケットの個数を、計数する計数手段，
前記計数手段が計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別手段，及び、
前記判別手段が前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティングループの発生の兆候がある旨を出力する出力手段
として機能させる
ことを特徴とするルーティングループ検出プログラム。
【請求項４】
コンピュータが、
ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出ステップと、
前記パケット抽出ステップにおいて抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先ＩＰアドレスを読み取る読取ステップと、
前記読取ステップにおいて読み取った送信先ＩＰアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信ステップと、
前記パケット送信ステップにおいて送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信ステップと、
前記パケット受信ステップにおいて受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティングループが発生している旨を出力する出力ステップと
を実行する
ことを特徴とするルーティングループ検出方法。
【請求項５】
コンピュータが、
ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をＩＰヘッダ中に有するパケットの個数を、計数する計数ステップと、
前記計数ステップにおいて計数したホップ数毎のパケットの個数に基づくヒストグラム

において、平坦部又は鋸歯状部の有無を判別する判別ステップと、
　前記判別ステップにおいて前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティングループの発生の兆候がある旨を出力する出力ステップと
を実行する
ことを特徴とするルーティングループ検出方法。

【書類名】明細書
【発明の名称】ルーティングループ検出プログラム及びルーティングループ検出方法
【技術分野】
【０００１】
本発明は、ルーティングループを検出するための装置としてコンピュータを機能させるルーティングループ検出プログラムと、このようなルーティングループ検出プログラムが実行されたコンピュータにより実現されるルーティングループ検出方法とに、関する。
【背景技術】
【０００２】
周知のように、インターネットやイントラネット等におけるネットワーク層プロトコルとして、ＴＣＰ／ＩＰ[Transmission Control Protocol／Internet Protocol]スイートに含まれるＩＰが、広く利用されている。
【０００３】
このＩＰに従った通信機能を有するコンピュータには、他のコンピュータの中から個別に識別するためのＩＰアドレスが、少なくとも１つ与えられている。この種のコンピュータは、ＯＳＩ［Open System Interconnection］参照モデルにおけるネットワーク層においてデータを送信する際、その送信データを、パケットと呼ばれる（データグラムとも言う）小さなデータの塊に分割し、送信元及び送信先のＩＰアドレスやその他の情報をヘッダ情報として各パケットに組み込んで、送信先のコンピュータへ向けて送信する。
【０００４】
また、この種のコンピュータは、同種の他のコンピュータと直接接続されていることは少なく、通常、パケットの中継を専門に行う複数のコンピュータを介して接続されている。この中継専門のコンピュータは、一般に、ルータと称されており、これらルータにも、ＩＰアドレスが与えられている。
【０００５】
各ルータは、パケットの送信先ＩＰアドレスとそのパケットの送信を担当する他のルータやコンピュータのＩＰアドレスとを対応付けたルーティングテーブルを、有しており、他のルータやコンピュータからパケットを受信すると、そのルーティングテーブルを参照して、次にパケットを送り渡すルータやコンピュータを選定して送信する。この結果、パケットは、幾つかのルータを経由して送信元のコンピュータから送信先のコンピュータへと順次送られる。
【０００６】
また、各ルータは、他のルータやコンピュータからパケットを受信すると、そのパケットのＩＰヘッダ中の所定フィールド（ＩＰバージョン４では生存時間、ＩＰバージョン６ではホップリミット）に記録される残存ホップ数から１を減じるとともに、ＩＰバージョン４に限りチェックサムフィールドの値を１増加させて、そのパケットを次のルータやコンピュータへ送信する。さらに、各ルータは、残存ホップ数が０になったパケットを破棄してパケット破棄の旨をＩＣＭＰ[Internet Control Message Protocol]に従って送信元ＩＰアドレスのコンピュータへ通知する処理も行う。
【０００７】
このようなルータやコンピュータによってＩＰに従ったパケット通信をネットワーク層において行うことができるネットワークは、一般に、ＩＰネットワークと称されている。
【０００８】
ところで、このＩＰネットワークにおいて生じる通信障害の一つに、ルーティングループがある。このルーティングループは、パケットが複数のルータ間を繰り返し巡回することによって送信先に届かなくなるという現象である。
【０００９】
このルーティングループは、手作業により行われる各種設定の間違いやルータ等のハードウエアの故障やその他の障害に因り生じてしまうことが多いが、そのルーティングループを引き起こしているルータ群を管理する管理者の管理区域外のルータの設定に因って引

き起こされることもある。通常、管理区域外のルータの設定を確認又は変更することはできないので、結局のところ、ルーティングループは防ぎようのない現象となっている。

【００１０】

そこで、このようなルーティングループの発生に因って管理者に及ぼされる損害を低く抑えるためには、ルーティングループを発生させているルータ群を如何に素早く発見するかが、重要となってくる。

【００１１】

従来、このようなルーティングループを発見するため、以下に説明する３つの方法が知られていた。

【００１２】

第１の方法は、ルーティングテーブルを用いる方法である。すなわち、この第１の方法は、管理区域内の全ルータの有するルーティングテーブルを付き合わせてループを形成しているエントリーレコードの組み合わせを１つずつ探し出すという方法である。この第１の方法には、ループを形成している組み合わせを確実に検出できるという利点がある。

【００１３】

第２の方法は、トレースルートを用いる方法である。すなわち、この第２の方法は、トレースルート機能を有するコンピュータを管理区域内のルータに接続してそのコンピュータから管理区域内の別のコンピュータへ残存ホップ数が１ずつ異なる調査用のパケットを順次送信するという方法である。この第２の方法では、当該コンピュータは、送信先のコンピュータまでの経路に存在する各ルータから送られてくる時間超過メッセージ付きパケット（タイプフィールドに１１を持つＩＣＭＰヘッダがＩＰヘッダに付加されたパケット）のうち、同じルータ群から繰り返し送られてきたものがある場合、そのルータ群においてルーティングループが発生していると検出する。この第２の方法には、管理区域内の全ての経路においてルーティングループを検出できるという利点がある。

【００１４】

第３の方法は、パケットキャプチャを用いる方法である。すなわち、この第３の方法は、パケットキャプチャ機能を有するコンピュータを管理区域内のルータ間に設置してそのルータ間を通過する全てのパケットを監視するという方法である（例えば非特許文献１参照）。この第３の方法では、当該コンピュータは、ＩＰヘッダ中の残存ホップ数（ＩＰバージョン４の場合にはチェックサム値も）以外の内容が同一であるパケットをそれぞれ抽出し、抽出した各パケットの残存ホップ数（及びチェックサム値）が等差数列的に変化している場合に、ルーティングループが発生していると検出する。この第３の方法には、即時にルーティングループを検出できるという利点がある。

【非特許文献１】ウルス＝ヘンガルトナー（Urs Hengartner），スー＝ムーン（Sue Moon），リチャード＝モルティエ（Richard Mortier），クリストフ＝ダイオット（Christophe Diot），“パケット経路中のルーティングループの検出と解析（Detection and Analysis of Routing Loops in Packet Traces）”，第３頁第４章ルーティングループの検出（IV Routing Loop Detection），[online]，平成１５年６月９日，インターネット＜ＵＲＬ：http://www-2.cs.cmu.edu/People/uhengart/imw02.pdf＞

【発明の開示】

【発明が解決しようとする課題】

【００１５】

しかしながら、上述した第１の方法によると、エントリーレコードの組み合わせを１つずつ手作業にて確認せねばならないため、ルーティングループが発見されるまでに非常に時間がかかる。また、通常のルーティングテーブルのエントリー数が例えば１００個のように非常に多いため、管理区域内のルータの数が増えれば増えるほど、ルーティングループを探し出す作業には、時間と手間が掛かることとなる。従って、この第１の方法は、即時性及び規模拡張性に優れないという問題があった。

【００１６】

また、上述した第２の方法によると、或る送信元ＩＰアドレスからのパケットだけがルーティングループを引き起こしてその他のパケットは引き起こさないという現象が、ルーティングテーブルの一部の間違いによって引き起こされ得るが、この場合、いくら調査用のパケットを経路に流してもルーティングループを検出することができないことがある。また、調査用のパケットは極めて大量に必要であるため、調査間隔を短くすればするほど、ネットワークトラフィックに多大な負荷を与えることとなり、新たな通信障害を引き起こす虞がある。従って、この第２の方法は、確実性及び即時性に優れないという問題があった。

【００１７】

さらに、上述した第３の方法によると、パケットキャプチャを跨いでいるルータ間で発生するルーティングループについては確実に検出できるものの、パケットキャプチャを跨いでいないルータ間で発生するルーティングループについては、検出することができない。そのうえ、ルータ間の通信速度が向上すればするほど、パケットキャプチャが取得するパケット数が増加してコンピュータの処理が追いつかなくなるため、ｉＤＣ［internet Data Center］やＩＳＰ［Internet Service Provider］などのように通信速度が早い大規模な管理区域に対して、当該コンピュータを適用することができない。従って、この第３の方法は、確実性及び規模拡張性に優れないという問題があった。

【００１８】

本発明は、上述したような従来の事情に鑑みてなされたものであり、その課題は、ネットワークの規模の大小に拘わらずルーティングループを確実且つ即時に検出するための装置としてコンピュータを機能させるルーティングループ検出プログラムと、このようなルーティングループ検出プログラムが実行されたコンピュータにより実現されるルーティングループ検出方法とを、提供することにある。

【課題を解決するための手段】

【００１９】

上記の課題を解決するために、本発明の第１の態様によるルーティングループ検出プログラムは、以下のような構成を採用した。

【００２０】

すなわち、本発明の第１の態様によるルーティングループ検出プログラムは、コンピュータを、ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をＩＰヘッダ中に有するパケットの個数を、計数する計数手段，前記計数手段が計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別手段，及び、前記判別手段が前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティングループの発生の兆候がある旨を出力する出力手段として機能させることを、特徴としている。

【００２１】

また、上記の課題を解決するために、本発明の第２の態様によるルーティングループ検出プログラムは、以下のような構成を採用した。

【００２２】

すなわち、本発明の第２の態様によるルーティングループ検出プログラムは、コンピュータを、ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出手段，前記パケット抽出手段が抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先ＩＰアドレスを読み取る読取手段，前記読取手段が読み取った送信先ＩＰアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信手段，前記パケット送信手段が送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信手段，及び、前記パケット受信手段が受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティングループが発生している旨を出力する出力手段として機能させることを、特徴として

いる。

【００２３】

これらのように構成されるので、少なくとも２台のルータを備えるとともにルータ同士を隣接させる全ての経路にそれぞれパケットキャプチャ装置が組み込まれたネットワークにおいて、第１の態様によるルーティングループ検出プログラムが実行された第１のコンピュータに対し、各パケットキャプチャ装置がキャプチャするパケットを監視させ、第２の態様によるルーティングループ検出プログラムが実行された第２のコンピュータに対し、ネットワーク中の最上流側にあるゲートウエイルータの直後に配置されているパケットキャプチャ装置がキャプチャするパケットを監視させれば、以下のような効果がある。

【００２４】

すなわち、ルータ同士を隣接させる全ての経路にそれぞれパケットキャプチャ装置を組み込むことにより、どのルータ間においてルーティングループが発生しても、その兆候を確実に捕らえることができる。また、或る送信元ＩＰアドレスからのパケットだけがルーティングループを引き起こしてその他のパケットは引き起こさないという現象が生じた場合でも、そのルーティングループの発生の兆候を確実に捕らえることができる。

【００２５】

このとき、第１のコンピュータに対しては、キャプチャされたパケットから残存ホップ数のみを取得させてホップ数毎の度数値をカウントさせるようにしているので、ルータ間の通信速度が高い大規模なネットワークであっても、第１のコンピュータの処理が追いつかなくなるようなことがなくなる。このため、ネットワークの規模の大小に拘わらず、そのネットワーク内の何れかのルータ間で生ずるルーティングループの発生の兆候を、確実且つ即時に検出することができる。

【００２６】

なお、第１のコンピュータによって検出されるルーティングループの発生の兆候には、トレースルートやアタックのような意図的な操作にて生じたものと、意図的な操作ではない純粋な通信障害として生じたものとが、含まれており、第１のコンピュータによっては、両者を区別することはできない。しかし、第１のコンピュータがルーティングループの発生の兆候を検出したときには、その兆候を検出したパケットキャプチャ装置に対応するルータのＩＰアドレスを第２のコンピュータに通知させれば、その第２のコンピュータが、その通知をトリガーとして、発生源となるルータを含む経路でのルーティングループの発生を調査することができる。

【００２７】

その調査を開始した第２のコンピュータは、ゲートウエイルータを通過するパケットの中から、外部ネットワークへ流出しようとする時間超過メッセージ付きパケットを監視する。そして、その時間超過メッセージ付きパケットを取得した場合には、第２のコンピュータは、その時間超過メッセージ付きパケットを発生させる基となった破棄されたパケットが本来到達すべき送信先ＩＰアドレスを、その時間超過メッセージから読み出し、その送信先ＩＰアドレス宛へ、調査用パケットを送信する。その後、第２のコンピュータは、調査用パケットの応答として、時間超過メッセージ付きパケットが送られてくるか否かを監視し、送られてきた場合には、そのパケットの送信元ＩＰアドレスが、第１のコンピュータから通知されたルータのものであるか否かを確認することができる。

【００２８】

このような調査を行う第２のコンピュータに対しては、ゲートウエイルータ直後の経路を通過するパケットの中から、時間超過メッセージを含むパケットだけを取得させるようにしている。この時間超過メッセージ付きパケットは、ルーティングループによるものの他に、トレースルートやアタックによるものも含まれるが、大きなネットワークにおいては、全パケット中の数割から数パーセントにしか過ぎない。然も、上述した第３の方法のように、パケットの内容が同一であるか否かをいちいち確認しない。このように、第２のコンピュータは、間引かれたパケットについて非常に簡単な処理しか行わなくて済むので、ゲートウエイルータ直後のような行き交うパケットの数が非常に膨大な大規模なネット

ワークであっても、時間超過メッセージ付きパケットを確実に捕らえて処理を施すことができる。

【００２９】

また、この第２のコンピュータは、時間超過メッセージ付きパケットを取得したときのみ、調査用パケットを送信するので、ネットワークの規模の大小とは無関係に、ネットワークトラフィックに負荷を掛けることがない。然も、このような時間超過メッセージ付きパケットを取得する処理は、第１のコンピュータからの通知を受けたときにしか行わない。従って、ゲートウエイルータ直後の経路には、殆ど負荷が掛かることがない。

【００３０】

以上を纏めると、本発明によれば、互いに隣接するルータ同士を繋ぐ全ての経路において、ホップ数毎の度数値からなるヒストグラムが監視され、そのヒストグラムにルーティングループの発生の兆候が現れた時には、時間超過メッセージ付きパケットの監視と調査用パケットの送信とにより、その兆候の発生源となるルータが検出されるので、確実にルーティングループを検出することができる。

【００３１】

また、本発明によれば、第１のコンピュータに対しては、キャプチャされたパケットからホップ数のみを取得させ、第２のコンピュータに対しては、時間超過メッセージ付きパケットを監視させているだけであるので、規模の大きなネットワークに適用した場合でも、これら第１及び第２のコンピュータが処理を即時に行うことができる。従って、ネットワークの規模の大小とは無関係に、ルーティングループを即時に検出することができる。

【００３２】

なお、本発明においては、調査用パケットは、アプリケーション層上に存在するネットワークアプリケーションサービスについてのサービス要求パケットであっても良いし、エコー要求メッセージを含むパケットであっても良い。

【００３３】

前者のようなサービス要求パケットの場合、ＩＰヘッダが付加されるセグメント内のレイヤ４ヘッダにおけるポート番号フィールドの値は、調査用パケットの送り先のノードにおいて開かれているネットワークアプリケーションサービスのポート番号に一致させておくと良い。こうしておくと、そのノードに至るまでの経路の途中においてパケットフィルタリングが行われていても、そのパケットフィルタリングによって調査用パケットが経路の途中で破棄されることがない。

【００３４】

また、本発明においては、調査用パケットの送り先は、時間超過メッセージから読み取られた破棄対象パケットの送信先ＩＰアドレスであるが、この調査用パケットのプロトコル番号は、この破棄対象パケットのプロトコル番号と一致していると良い。このように、プロトコル番号を一致させる方法としては、そのプロトコル番号を、時間超過メッセージから送信先ＩＰアドレスとともに読み出しておけば良い。このように、調査用パケットに対してプロトコル番号を動的に付与するようにしておくと、調査用パケットの送り先に至るまでの各ルータにおいて動作中の通信サービスのプロトコル番号を、いちいち確認しなくても済むようになる。

【００３５】

また、本発明においては、調査用パケットは、所定のパケット送信プログラムによって動的に作成されるものであっても良いが、事前に記憶装置に記憶されていて必要がある場合に読み出されるものであっても良い。後者のように記憶装置に調査用パケットを記憶しておく場合、その調査用パケットは、調査において不変な情報を所定のフィールドに既に有するものであると良い。こうしておくと、調査用パケットが必要となった場合には、記憶装置から読み出してその所定のフィールドの内容を調査において必要な情報で更新するだけで済むので、パケット送信プログラムをいちいち立ち上げて処理を行わせるような負荷をコンピュータに与えることがなくなる。従って、時間超過メッセージの監視や調査用パケットの送信に係る処理速度をできるだけ高速化することができる。

【００３６】
また、本発明は、時間超過メッセージから読み取られる送信先ＩＰアドレスが同一サブネット中のノードを示すものである場合に、その調査用パケットをそれらノードへ繰り返し送信するものであっても良いが、同一サブネット中の１つのノードへ一旦調査用パケットを送信した後、所定期間が経過するまで、そのサブネット中の各ノードへは調査用パケットを送信しないものであっても良い。こうしておくと、ルーティングループやトレースルートやアタックによって同一内容の時間超過メッセージ付きパケットが短期間に大量発せられる場合であっても、それらについていちいち調査用パケットを生成することが無くなる。そのため、調査回数を抑えることができ、その結果、ネットワークトラフィックに掛かる負荷を軽減することができる。
【００３７】
また、本発明は、時間超過メッセージ付きパケットを取得すると、調査対象となるノードが有する様々な条件とは無関係に、そのノードに調査用パケットを送信するものであっても良いが、調査対象となるノードが有する諸条件に応じて調査用パケットを取り止めるものであっても良い。こうしておくと、ルーティングループからの復旧作業中にあるルータや、破棄パケットのプロトコル番号の示すサービスが実際には作動していないノードに関する条件を事前に設定しておけば、不要な調査用パケットをネットワークに流さなくて済むので、ネットワークトラフィックに掛かる負荷を軽減することができる。
【００３８】
また、本発明は、調査用パケットの送信に対する応答として時間超過メッセージ付きパケットを受け取ったコンピュータに対し、さらに、トレースルートの手法によって、ルーティングループを生じさせているルータ及びそのルータに至るまでの経路を特定させるものであっても良い。こうしておくと、ルーティングループを生じさせているルータを確実に特定することができるようになる。
【００３９】
また、上記の課題を解決するために、本発明の第１の態様によるルーティングループ検出方法は、以下のような構成を採用した。
【００４０】
すなわち、本発明の第１の態様によるルーティングループ検出方法は、コンピュータが、ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をＩＰヘッダ中に有するパケットの個数を、計数する計数ステップと、前記計数ステップにおいて計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別ステップと、前記判別ステップにおいて前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティングループの発生の兆候がある旨を出力する出力ステップとを実行することを、特徴としている。
【００４１】
また、上記の課題を解決するために、本発明の第２の態様によるルーティングループ検出方法は、以下のような構成を採用した。
【００４２】
すなわち、本発明の第２の態様によるルーティングループ検出方法は、コンピュータが、ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出ステップと、前記パケット抽出ステップにおいて抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先ＩＰアドレスを読み取る読取ステップと、前記読取ステップにおいて読み取った送信先ＩＰアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信ステップと、前記パケット送信ステップにおいて送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信ステップと、前記パケット受信ステップにおいて受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティングループが発生している旨

を出力する出力ステップとを実行することを、特徴としている。

【００４３】

従って、これら第１及び第２の態様によるルーティングループ検出方法は、上述した本発明の第１及び第２の態様によるルーティングループ検出プログラムが実行されたコンピュータにより実現されることになる。

【発明の効果】

【００４４】

以上に説明したように、本発明によれば、ネットワークの規模の大小に拘わらずルーティングループを確実且つ即時に検出することができる。

【発明を実施するための最良の形態】

【００４５】

本発明は、或る管理組織が同一の管理ポリシーに従って運用しているネットワーク（いわゆるＡＳ［Autonomous System］）に対して、適用される。すなわち、本発明は、ｉＤＣ[internet Data Center]の管理するネットワーク，ＩＳＰ［Internet Service Provider］の管理するネットワーク，企業及び学術団体のイントラネット，ＷＡＮ［Wide Area Network］，並びに、ＬＡＮ［Local Area Network］などに対して、適用される。以下では、本発明を実施するための形態の一例として、いわゆるハウジング（コロケーションとも言う）方式にて顧客に対して通信回線やサーバシステムの設置場所を提供するｉＤＣが管理するネットワークに対して本発明を適用した例を、図面に基づいて説明する。

【００４６】

図１は、本発明が適用されたネットワークＮを概略的に示す構成図である。図１に示されるように、このネットワークＮは、複数のルータ１０を備えている。各ルータ１０は、所定の通信ケーブルを介して接続されており、全体として、ツリー型のネットワークを形成している。なお、このツリーのトップが上流側である。

【００４７】

このネットワークＮを構成している各ルータ１０のうち、最下流のルータ１０には、ｉＤＣの顧客の管理下にあるサーバシステム２０が、接続されている。各顧客のサーバシステム２０は、その顧客が自ら構築したシステムであり、単独のサーバコンピュータから構成され、或いは、複数台のサーバコンピュータ，ルータ，スイッチングハブ等から構成される。

【００４８】

また、最上流のルータ１０は、いわゆるゲートウエイルータとして機能する。なお、他のルータ１０と区別するために、図１では、このゲートウエイルータの符号を１０’と表記している。このゲートウエイルータ１０’には、インターネットＩを構成する各ネットワーク（上述したＩＳＰ，ｉＤＳ，イントラネット，ＷＡＮ，ＬＡＮ）のゲートウエイルータ，或いは、これらゲートウエイルータの接続ポイントとして機能するＩＸ[Internet eXchange]が、高速通信線を介して接続されている。

【００４９】

また、このネットワークＮ内では、ＯＳＩ［Open System Interconnection］参照モデルのネットワーク層（レイヤ３）に相当するプロトコルとして、ＴＣＰ／ＩＰ[Transmission Control Protocol／Internet Protocol]スイートに含まれるＩＰ及びＩＣＭＰ［Internet Control Message Protocol］が、用られている。すなわち、このＩＰ及びＩＣＭＰに従った通信を行うためのプログラムが、各ルータ１０のＲＯＭ［Read Only Memory］等に搭載されている。

【００５０】

さらに、このネットワークＮは、本発明に係る第１のルーティングループ検出装置３０を、複数備えている。これら第１のルーティングループ検出装置３０は、図１に示されるように、互いに隣接するルータ１０同士の間に割り込まされることによって、それぞれ、一対のルータ１０，１０を連絡している。図２は、この第１のルーティングループ検出装置３０を概略的に示す構成図である。

【００５１】
第１のルーティングループ検出装置３０は、ＣＰＵ［Central Processing Unit］３０ａ，ＲＡＭ［Random Access Memory］３０ｂ，通信制御装置３０ｃ，及び、ＨＤＤ［Hard Disk Drive］３０ｄを、備えている。
【００５２】
ＣＰＵ３０ａは、この第１のルーティングループ検出装置３０全体を制御するための中央処理装置である。ＲＡＭ３０ｂは、ＣＰＵ３０ａが各種プログラムを実行するに際しての作業領域が展開される主記憶装置である。
【００５３】
通信制御装置３０ｃは、ＯＳＩ参照モデルのデータリンク層及び物理層に相当するプロトコルに従った通信を司る装置であり、上述したルータ１０における当該プロトコルに従った通信を司るデバイスと同等のデバイス（例えばスイッチングハブ）である。
【００５４】
ＨＤＤ３０ｄは、各種のプログラム及び各種のデータが格納される記憶装置である。このＨＤＤ３０ｄには、オペレーティングシステムプログラムの他、本発明に係る第１のルーティングループ検出プログラム３１，パケットキャプチャプログラム３２，及び、パケット送信プログラム３３が、格納されている。
【００５５】
第１のルーティングループ検出プログラム３１は、２つのモジュールプログラム３１ａ，３１ｂとこれらモジュールプログラム３１ａ，３１ｂの実行を制御するためのプログラムとを、含んでいる。この第１のルーティングループ検出プログラム３１に含まれる２つのモジュールプログラム３１ａ，３１ｂのうち、一方は、図５を用いて後述する集計プログラム３１ａであり、他方は、図６を用いて後述する解析プログラム３１ｂである。
【００５６】
パケットキャプチャプログラム３２は、ＯＳＩ参照モデルのネットワーク層に位置するプログラムであり、ＣＰＵ３０ａに対し、パケットをキャプチャさせるためのプログラムである。すなわち、パケットキャプチャプログラム３２は、通信制御装置３０ｃに対してそれに入力されたパケットを全て受け取らせて上位層へ引き渡させるとともに、受信したパケットと同じパケットを元の経路に戻させるためのプログラムである。なお、このパケットキャプチャプログラム３２は、ネットワークＮにおける上流側から下流側に向かって流れるパケットのみをキャプチャするように、設定されている。
【００５７】
パケット送信プログラム３３は、ＣＰＵ３０ａに対し、ネットワーク層より上位の層から引き渡されたセグメントをパケットにカプセル化して通信制御装置３０ｃへ引き渡させるためのプログラムである。
【００５８】
なお、パケットキャプチャプログラム３２を実行するＣＰＵ３０ａ，及び、通信制御装置３０ｃは、パケットキャプチャ装置に相当する。図２では、第１のルーティングループ検出プログラム３１とパケットキャプチャプログラム３２とが、一台のコンピュータに格納されているように、示されているが、別々のコンピュータに格納されていても良い。この場合、パケットキャプチャプログラム３２が格納されるコンピュータは、パケットキャプチャ装置として機能するために、通信制御装置３０ｃを備えることとなる。
【００５９】
さらに、このネットワークＮは、本発明に係る第２のルーティングループ検出装置４０を、備えている。この第２のルーティングループ検出装置４０は、図１に示されるように、ゲートウエイルータ１０’とこれに隣接する２個のルータ１０，１０との間に割り込まされることによって、これらルータ１０’，１０，１０を連絡している。図３は、この第２のルーティングループ検出装置４０を概略的に示す構成図である。
【００６０】
第２のルーティングループ検出装置４０は、ＣＰＵ４０ａ，ＲＡＭ４０ｂ，通信制御装

置４０ｃ，及び、ＨＤＤ４０ｄを、備えている。これらハードウエア４０ａ～４０ｄは、第１のルーティングループ検出装置３０のそれらと同等のハードウエアである。

【００６１】

但し、ＨＤＤ４０ｄには、第１のルーティングループ検出装置３０のＨＤＤ３０ｄに格納されているプログラムとは一部異なるプログラムが、格納されている。具体的には、ＨＤＤ４０ｄには、オペレーティングシステムプログラム，第２のルーティングループ検出プログラム４１，パケットキャプチャプログラム４２，及び、パケット受信プログラム４３が、格納されている。

【００６２】

第２のルーティングループ検出プログラム４１は、２つのモジュールプログラム４１ａ，４１ｂとこれらモジュールプログラム４１ａ，４１ｂの実行を制御するためのプログラムとを、含んでいる。この第２のルーティングループ検出プログラム４１に含まれる２つのモジュールプログラム４１ａ，４１ｂのうち、一方は、図１１を用いて後述する監視プログラム４１ａであり、他方は、図１２乃至図１４を用いて後述する調査プログラム４１ｂである。

【００６３】

パケットキャプチャプログラム４２は、第１のルーティングループ検出装置３０のそれと同様の機能を発揮するものである。但し、第２のルーティングループ検出装置４０のパケットキャプチャプログラム４２は、第１のルーティングループ検出装置３０のそれとは逆に、ネットワークＮにおける下流側から上流側に向かって流れるパケットのみをキャプチャするように、設定されている。なお、パケットキャプチャプログラム４２を実行するＣＰＵ４０ａ，及び、通信制御装置４０ｃは、パケットキャプチャ装置に相当する。従って、上述したのと同じ理由により、第２のルーティングループ検出プログラム４１とパケットキャプチャプログラム４２とは、同一のコンピュータに格納されていても良いし、別々のコンピュータに格納されていても良い。

【００６４】

パケット受信プログラム４３は、ＣＰＵ４０ａに対し、通信制御装置４０ｃから引き渡されたパケットからＩＰヘッダを取り除かせることによってセグメントを生成して上位層へ引き渡させるプログラムである。

【００６５】

次に、以上のように構成されるネットワークＮにおいて実行される処理について説明する。なお、以下では、先に、第１のルーティングループ検出装置３０において実行される処理の内容を説明して、その処理によってなされる作用効果を説明し、その後、第２のルーティングループ検出装置４０において実行される処理の内容を説明して、その処理によってなされる作用効果について説明する。

【００６６】

まず、第１のルーティングループ検出装置３０において実行される処理の内容について説明する。第１のルーティングループ検出装置３０では、主電源が投入されると、ＣＰＵ３０ａによってＨＤＤ３０ｄから第１のルーティングループ検出プログラム３１が読み出され、第１のルーティングループ検出処理が実行される。図４は、この第１のルーティングループ検出処理の内容を説明するためのフローチャートである。

【００６７】

第１のルーティングループ検出処理の開始後、最初のステップＳ１０１では、ＣＰＵ３０ａは、時間計測を開始し、ステップＳ１０２へ処理を進める。

【００６８】

ステップＳ１０２では、ＣＰＵ３０ａは、集計プログラム３１ａ及び解析プログラム３１ｂを実行する。つまり、第１のルーティングループ検出装置３０には、集計処理プロセス及び解析処理プロセスが、生成される。なお、集計処理プロセス及び解析処理プロセスは、並行に実行される。また、これら集計処理及び解析処理の内容については、図５及び図６を用いて後述する。これら二つのプロセスの生成後、ＣＰＵ３０ａは、ステップＳ１

０３へ処理を進める。

【００６９】

ステップＳ１０３では、ＣＰＵ３０ａは、解析処理プロセスが消滅するまで待機する（Ｓ１０３；ＮＯ）。そして、解析処理プロセスが消滅すると（Ｓ１０３；ＹＥＳ）、ＣＰＵ３０ａは、ステップＳ１０４へ処理を進める。

【００７０】

ステップＳ１０４では、ＣＰＵ３０ａは、兆候検出フラグが１であるか否かを判別する。なお、この兆候検出フラグは、解析処理プロセスの実行の結果、０及び１の何れかに切り替えられる。そして、ＣＰＵ３０ａは、兆候検出フラグが１でなかった場合（Ｓ１０４；ＮＯ）には、ステップＳ１０６へ進め、兆候検出フラグが１であった場合（Ｓ１０４；ＹＥＳ）には、ステップＳ１０５へ処理を進める。

【００７１】

ステップＳ１０５では、ＣＰＵ３０ａは、この第１のルーティングループ検出装置３０が割り込まされている検査対象の経路について、その両端のルータのＩＰアドレスと、ルーティングループの発生の兆候が検出された旨とを含む兆候通知を、第２のルーティングループ検出装置４０へ送信する。なお、この送信では、パケット送信プログラム３３による機能が用いられる。送信後、ＣＰＵ３０ａは、ステップＳ１０６へ処理を進める。

【００７２】

ステップＳ１０６では、ＣＰＵ３０ａは、ステップＳ１０１における時間計測の開始時点から所定時間（例えば１０分）が経過するまで待機する（Ｓ１０６；ＮＯ）。そして、時間計測の開始時点から所定時間が経過すると（Ｓ１０６；ＹＥＳ）、ＣＰＵ３０ａは、ステップＳ１０１へ処理を戻し、新たに、集計処理プロセスと解析処理プロセスを生成する。

【００７３】

従って、第１のルーティングループ検出装置３０では、主電源が投入されている間、ステップＳ１０２～Ｓ１０５が、定期的に実行される。

【００７４】

図５は、集計処理の内容を説明するためのフローチャートである。この集計処理の開始後、最初のステップＳ１１１では、ＣＰＵ３０ａ（以下、ＣＰＵ３０ａが集計プログラム３１ａを実行することによって実現される機能を、集計処理プロセス３１ａと表記する）は、時間計測を開始し、ステップＳ１１２へ処理を進める。

【００７５】

ステップＳ１１２では、集計処理プロセス３１ａは、パケットキャプチャプログラム３２（を実行したＣＰＵ３０ａによる機能）から１個のパケットのデータを受け取ったか否かを、判別する。そして、集計処理プロセス３１ａは、パケットキャプチャプログラム３２から１個のパケットのデータを受け取っていなかった場合（Ｓ１１２；ＮＯ）には、ステップＳ１１５へ処理を進め、パケットキャプチャプログラム３２から１個のパケットのデータを受け取っていた場合（Ｓ１１２；ＹＥＳ）には、ステップＳ１１３へ処理を進める。

【００７６】

ステップＳ１１３では、集計処理プロセス３１ａは、このパケットのＩＰヘッダ中の生存時間フィールド（ＩＰバージョン６の場合にはホップリミットフィールド）から残存ホップ数を読み取り、ステップＳ１１４へ処理を進める。

【００７７】

ステップＳ１１４では、集計処理プロセス３１ａは、読み取った残存ホップ数の値を解析処理プロセスへ通知し、ステップＳ１１５へ処理を進める。

【００７８】

ステップＳ１１５では、集計処理プロセス３１ａは、時間計測を開始してから所定時間（例えば１０秒）が経過したか否かを、判別する。そして、所定時間が経過していなかった場合（Ｓ１１５；ＮＯ）には、集計処理プロセス３１ａは、ステップＳ１１２へ処理を

戻す。

【００７９】

このステップＳ１１２～Ｓ１１５の処理ループでは、上流から下流に向かいながら第１ルーティングループ検出装置３０を通過する全てのパケットの残存ホップ数が、順次、解析処理プロセス３１ｂへ通知される。そして、この処理ループの実行中、時間計測を開始してから所定時間が経過した場合には、集計処理プロセス３１ａは、ステップＳ１１５からＳ１１６へ処理を分岐させる（Ｓ１１５；ＹＥＳ）。

【００８０】

ステップＳ１１６では、集計処理プロセス３１ａは、解析処理プロセス３１ｂへ監視終了を通知し、集計処理を終了する。

【００８１】

図６は、解析処理の内容を説明するためのフローチャートである。解析処理の開始後、最初のステップＳ１２１では、ＣＰＵ３０ａ（以下、ＣＰＵ３０ａが解析プログラム３１ｂを実行することによって実現される機能を、解析処理プロセス３１ｂと表記する）は、ＲＡＭ３０ｂ内のワークテーブルを初期化するとともに、兆候検出フラグを０に切り替えることによって当該フラグを初期化する。

【００８２】

なお、ワークテーブルは、ＩＰヘッダの生存時間フィールド（ＩＰバージョン６の場合にはホップリミットフィールド）において取り得るホップ数（２５５）と同じ数のレコードを、有する。各レコードは、ホップ数のフィールドと、そのホップ数を残存ホップ数として有するパケットの個数を示す度数値のフィールドとを、含んでいる。

【００８３】

このステップＳ１２１では、解析処理プロセス３１ｂは、このワークテーブル中の全てのレコードの度数値フィールドを０にリセットすることによって、ワークテーブルを初期化する。ワークテーブル及び兆候検出フラグの初期化後、解析処理プロセス３１ｂは、ステップＳ１２２へ処理を進める。

【００８４】

ステップＳ１２２では、解析処理プロセス３１ｂは、集計処理プロセス３１ａから残存ホップ数の値が通知されているか否かを、判別する。そして、解析処理プロセス３１ｂは、集計処理プロセス３１ａから残存ホップ数の値が通知されていなかった場合（Ｓ１２２；ＮＯ）には、ステップＳ１２４へ処理を進め、集計処理プロセスから残存ホップ数の値が通知されていた場合（Ｓ１２２；ＹＥＳ）には、ステップＳ１２３へ処理を進める。

【００８５】

ステップＳ１２３では、解析処理プロセス３１ｂは、ワークテーブルにおける当該ホップ数に対応する度数値を１つカウントアップし、ステップＳ１２４へ処理を進める。

【００８６】

ステップＳ１２４では、解析処理プロセス３１ｂは、集計処理プロセス３１ａから監視終了が通知されているか否かを、判別する。そして、集計処理プロセス３１ａから監視終了が通知されていなかった場合（Ｓ１２４；ＮＯ）には、解析処理プロセス３１ｂは、ステップＳ１２２へ処理を戻す。

【００８７】

このステップＳ１２２～Ｓ１２４の処理ループでは、集計処理プロセス３１ａから通知される各パケットの残存ホップ数に基づいて、ワークテーブル内の度数値を順次カウントアップする。そして、この処理ループの実行中、集計処理プロセス３１ａから監視終了が通知された場合には、解析処理プロセス３１ｂは、ステップＳ１２４からＳ１２５へ処理を分岐させる（Ｓ１２４；ＹＥＳ）。

【００８８】

ステップＳ１２５では、解析処理プロセス３１ｂは、ワークテーブル中の各ホップ数とその度数値とに基づいて、度数分布グラフ（ヒストグラム）の曲線における平坦部（又は鋸歯状部）に相当する部分の有無を、検索する。

【００８９】
ここで、ワークテーブル中の各ホップ数とその度数値とに基づいて生成され得るヒストグラムについて、簡単に説明する。図７は、ルーティングループが発生していない場合でのヒストグラムの一例を示し、図８は、ルーティングループが発生している場合でのヒストグラムの一例を示す。なお、図７及び図８では、度数値の軸は、対数軸となっている。
【００９０】
ルーティングループが発生していない場合、図７に示されるように、ヒストグラムには、幾つかのピークが形成されているとともに、各ピークの脇には、なだらかな曲線状の裾野が形成されている。なお、ピークが出現するのは、パケットに付与する最大ホップ数として各種のＯＳ［Operation System］や装置に設定されているデフォルト値に起因する。デフォルト値としてよく知られているものとして、例えば、windows（マイクロソフト社商標）系は１２８、Linux系は６４、MacOS（アップルコンピュータ社商標）系は６４と２５５、ルータは２５５である。図７においても、ホップ数が１２８や２５５である地点の近辺に、ピークが出現している。
【００９１】
一方、ルーティングループが発生している場合、図８に示されるように、ヒストグラムには、図７の場合と同様に、幾つかのピークが形成されているが、各ピークの裾野は、ほぼ平坦になっている。このようにピークの裾野が平坦となるのは、以下の理由に因る。
【００９２】
すなわち、隣接するルータ同士で一つのパケットを送受信し続けるという現象がルーティングループとして最も多く出現するパターンであるが、このパターンでは、第１のルーティングループ検出装置３０は、…，１２５，１２３，１２１，１１９，…のように、同一のパケットについて２つずつ異なる残存ホップ数をそれぞれ取得することとなる。勿論、３つ以上のルータに跨るようにルーティングループが発生した場合には、第１のルーティングループ検出装置３０は、等差数列的に値が異なる残存ホップ数をそれぞれ取得することとなる。何れにしても、複数のパケットが同一ルータ間でルーティングループを発生させた場合には、ヒストグラムにおけるホップ数のグラフ軸における離散的な地点（上記の例で言えば、…，１２５，１２３，１２１，１１９，…の地点）の度数値が、それらパケットの個数と同じ数になる。このとき、ヒストグラムにおけるピークの裾野は、図９に示されるように、鋸歯状となる。なお、このようにピークの裾野が鋸歯状となるためには、ルーティングループに突入する前の各パケットが同じ残存ホップ数（或いは、上記の例で言えば奇数の残存ホップ数）を持っていなければならないが、現実には、各パケットの持つ残存ホップ数が揃っていないことが多い。このように残存ホップ数が揃っていなかった場合には、ヒストグラムにおける各ホップ数での度数値は、平均的になる。その結果、ルーティングループが発生している場合でのピークの裾野は、概ね平坦になる。
【００９３】
そして、図６のステップＳ１２５では、上述したようなヒストグラムにおける平坦部（又は鋸歯状部）に相当する部分の有無が検索されるが、その検索方法については、様々な手法が知られており、その一例としては、以下のような手法がある。
【００９４】
すなわち、その手法を概念的に説明すると、まず、ヒストグラムの度数値の軸を所定数（例えば５）ずつの区間に区分することによって、グラフ曲線を構成する２５５個のデータを各区間に振り分け、その後、各区間のうち、含まれるデータ数が所定の閾値を超えた区間が存在するか否かを、判別する。そして、所定の閾値を超えた区間が存在した場合に、ヒストグラムに平坦部（又は鋸歯状部）が存在するとして検出する。
【００９５】
次のステップＳ１２６では、解析処理プロセス３１ｂは、ヒストグラムにおける平坦部（鋸歯状部）に相当する部分が検出できたか否かを、判別する。そして、解析処理プロセス３１ｂは、ヒストグラムにおける平坦部（鋸歯状部）に相当する部分が検出できなかった場合（Ｓ１２６；ＮＯ）には、解析処理を終了し、ヒストグラムにおける平坦部（鋸歯

状部）に相当する部分が検出できた場合（Ｓ１２６；ＹＥＳ）には、ステップＳ１２７へ処理を進める。

【００９６】

ステップＳ１２７では、解析処理プロセス３１ｂは、兆候検出フラグを１に切り替えて、解析処理を終了する。

【００９７】

以上に説明した第１のルーティングループ検出処理が実行されることにより、第１のルーティングループ検出装置３０は、以下に説明するように作用する。

【００９８】

第１のルーティングループ検出装置３０が割り込まされた経路を上流側から下流側に向かって送信される全てのパケットは、第１のルーティングループ検出装置３０においてキャプチャされる。そして、第１のルーティングループ検出装置３０において解析処理プロセス３１ｂが生成されている期間（Ｓ１０１，Ｓ１０２，Ｓ１０６）において、集計処理プロセス３１ａが生成されている期間にあるとき（Ｓ１１１，Ｓ１１５）には、キャプチャされた全てのパケットの残存ホップ数が読み取られ（Ｓ１１２～Ｓ１１４）、それに基づいてワークテーブルが生成される（Ｓ１２２，Ｓ１２３）。そして、集計処理プロセス３１ａによる残存ホップ数の読み取り期間が終了すると（Ｓ１１５；ＹＥＳ，Ｓ１１６，Ｓ１２４；ＹＥＳ）、ワークテーブル中の各ホップ数とその度数値とに基づいて、ヒストグラムの曲線における平坦部（又は鋸歯状部）に相当する部分の有無が検索され（Ｓ１２５）、ヒストグラムの曲線における平坦部（又は鋸歯状部）に相当する部分が検出されると（Ｓ１２６；ＹＥＳ）、この第１のルーティングループ検出装置３０が割り込まされた経路の両端にあるルータのＩＰアドレスとともに、兆候通知が第２のルーティングループ検出装置４０へ送信される（Ｓ１０５）。

【００９９】

つまり、この第１のルーティングループ検出装置３０では、主電源が投入されている間、このような全パケットの残存ホップ数の一定期間での読み取り（Ｓ１１１～Ｓ１１６，Ｓ１２２～Ｓ１２４）と、読み取った残存ホップ数に基づく兆候通知の送信の可否の判定（Ｓ１２５～Ｓ１２７，Ｓ１０３～Ｓ１０５）とが、定期的に繰り返される（Ｓ１０１，Ｓ１０２，Ｓ１０６）。

【０１００】

このように作用するために、第１のルーティングループ検出装置３０は、以下に説明するような効果を奏する。

【０１０１】

すなわち、従来の方法（上述した第３の方法）によれば、監視対象となるパケット全てについて同一内容か否かを一つ一つ検査する必要があった。この検査に必要な１パケット当たりのデータ量は、ＩＰバージョン４においては、１３バイト（＝識別情報(２バイト)＋生存時間(１バイト)＋ヘッダチェックサム(２バイト)＋送信元ＩＰアドレス(４バイト)＋送信先ＩＰアドレス(４バイト)）であり、ＩＰバージョン６においては、３６バイト（＝フローラベル(３バイト)＋ホップリミット(１バイト)＋送信元ＩＰアドレス(１６バイト)＋送信先ＩＰアドレス(１６バイト)）である。しかし、本実施形態の第１のルーティングループ検出装置３０は、全パケットを監視することにはなるとしても、単に各パケットから残存ホップ数（１バイト）を読み取っているだけであり、且つ、ワークテーブル内の度数値をカウントアップさせるという簡易な処理を実行するだけである。然も、全パケットにおける全ての組み合わせについて互いにマッチングするか否かを判別するというような重い処理も行わない。このため、パケットの流入量が非常に膨大であっても、パケットキャプチャ時に、第１のルーティングループ検出装置３０には、処理負荷が殆ど掛からない。つまり、第１のルーティングループ検出装置３０は、隣接するルータ同士を繋ぐ通信回線の通信速度が高速であったとしても、すなわち、大規模なネットワークに適用されたとしても、適切に処理を行える。

【０１０２】

また、トレースルートによって検出できないルーティングループ、すなわち、或る送信元から送られたパケットだけがルーティングループを生じさせてその他のパケットはルーティングループを生じさせないというようなルーティングループであっても、そのルーティングループが第１のルーティングループ検出装置３０を跨いでいれば、その第１のルーティングループ検出装置３０によって確実に検出される。然も、互いに隣接するルータ同士を繋ぐ全ての経路に対し、第１のルーティングループ検出装置３０が割り込まされていることにより、管理区域内で生ずるルーティングループは、何れかの第１のルーティングループ検出装置３０を必ず跨ぐこととなるので、管理区域内で生ずるルーティングループは、確実に検出されることとなる。

【０１０３】

但し、ヒストグラムにおける平坦部（又は鋸歯状部）は、ルーティングループを生じさせているパケットの他に、トレースルートのために送信されてきた多量のパケットや、互いに異なる残存ホップ数を持ちつつアタックとして送り付けられた多量のパケットによっても、生成される。つまり、ルーティングループが発生すれば、必ずヒストグラムに平坦部（又は鋸歯状部）が生じるものの、ヒストグラムにおける平坦部（又は鋸歯状部）が、必ずしもルーティングループを示している訳ではない。従って、第１のルーティングループ検出装置３０は、少なくとも、ルーティングループの発生の兆候を見逃さないと言うことができる。

【０１０４】

さらに、第１のルーティングループ検出装置３０では、兆候通知の送信の可否の判定を行う時間間隔（Ｓ１０６）を例えば１時間のように長めに設定しておけば、第１のルーティングループ検出装置３０に掛かる処理の負荷やこのネットワークＮのトラフィックに掛かる負荷をできるだけ抑えることができ、逆に、その時間間隔を例えば１分のように短めに設定しておけば、ルーティングループの発生を即時に検出することができる。なお、何れの場合でも、パケットから残存ホップ数を読み取る期間（Ｓ１１５）よりも、兆候通知の送信の可否の判定を行う時間間隔（Ｓ１０６）を短めに設定することが望ましい。

【０１０５】

次に、第２のルーティングループ検出装置４０において実行される処理の内容について説明する。第２のルーティングループ検出装置４０では、何れかの第１のルーティングループ検出装置３０から兆候通知が、パケット受信プログラム４３の機能を通じて受信されると、それをトリガーとして、ＣＰＵ４０ａによってＨＤＤ４０ｄから第２のルーティングループ検出プログラム４１が読み出され、第２のルーティングループ検出処理が実行される。図１０は、この第２のルーティングループ検出処理の内容を説明するためのフローチャートである。

【０１０６】

第２のルーティングループ検出処理の開始後、最初のステップＳ２０１では、ＣＰＵ４０ａは、監視プログラム４１ａを実行する。つまり、第２のルーティングループ検出装置４０には、監視処理プロセスが生成される。

【０１０７】

図１１は、監視処理の内容を説明するためのフローチャートである。監視処理の開始後、最初のステップＳ２１１では、ＣＰＵ４０ａ（以下、ＣＰＵ４０ａが監視プログラム４１ａを実行することによって実現される機能を、監視処理プロセス４１ａと表記する）は、パケットキャプチャプログラム４２（を実行したＣＰＵ４０ａによる機能）から１個のパケットのデータを受け取るまで、待機する（Ｓ２１１；ＮＯ）。そして、パケットキャプチャプログラム４２から１個のパケットのデータを受け取ると（Ｓ２１１；ＹＥＳ）、監視処理プロセス４１ａは、ステップＳ２１２へ処理を進める。

【０１０８】

ステップＳ２１２では、監視処理プロセス４１ａは、このパケットが時間超過メッセージ付きパケットであるか否かを、判別する。なお、時間超過メッセージとは、タイプフィールドに１１を持つＩＣＭＰヘッダのことである。このステップＳ２１２における処理を

具体的に説明すると、監視処理プロセス４１ａは、ステップＳ２１１においてキャプチャしたパケットがＩＰヘッダのプロトコル番号フィールドに１を持つか否かを、まず判別し、プロトコル番号フィールドに１を持つ場合には、ＩＰヘッダにはＩＣＭＰヘッダが付加されているので、そのＩＣＭＰヘッダのタイプフィールドが１１であるか否かを判別する。そして、監視処理プロセス４１ａは、プロトコル番号が１でない場合、或いは、プロトコル番号が１であるがタイプフィールドが１１でない場合、キャプチャしたパケットに時間超過メッセージが含まれていないとして（Ｓ２１２；ＮＯ）、ステップＳ２１１へ処理を戻し、プロトコル番号が１であってタイプフィールドが１１である場合、キャプチャしたパケットに時間超過メッセージが含まれているとして（Ｓ２１２；ＹＥＳ）、ステップＳ２１３へ処理を進める。

【０１０９】

ステップＳ２１３では、監視処理プロセス４１ａは、ステップＳ２１１において受信したパケットから、このパケットを発生させる基となったパケットの送信先のＩＰアドレスを読み取る。具体的には、時間超過メッセージとしてのＩＣＭＰヘッダのＩＣＭＰオプションフィールドには、この時間超過メッセージを生成する基となったパケット（すなわち、その宛先に到達する前に残存ホップ数がゼロとなって破棄されてしまったパケット）のＩＰヘッダとセグメントの一部とが、コピーされており、監視処理プロセス４１ａは、このＩＣＭＰオプションフィールドから、本来の送信先ＩＰアドレスを読み取る。読み取り後、監視処理プロセス４１ａは、ステップＳ２１４へ処理を進める。

【０１１０】

ステップＳ２１４では、監視処理プロセス４１ａは、ステップＳ２１１において受信したパケットのＩＣＭＰオプションフィールドから、その時間超過メッセージを生成する基となったパケットがそのＩＰヘッダのプロトコル番号フィールドに持っていたプロトコル番号を読み取る。読み取り後、監視処理プロセス４１ａは、ステップＳ２１５へ処理を進める。

【０１１１】

ステップＳ２１５では、監視処理プロセス４１ａは、ステップＳ２１４において読み取ったプロトコル番号が６又は１７であるか否かを、判別する。すなわち、監視処理プロセス４１ａは、当該時間超過メッセージを生成する基となったパケットがＴＣＰヘッダ又はＵＤＰ［User Datagram Protocol］ヘッダを持っていたか否かを、判別する。そして、監視処理プロセス４１ａは、当該プロトコル番号が６又は１７でなかった場合（Ｓ２１５；ＮＯ）には、ステップＳ２１７へ処理を進め、当該プロトコル番号が６又は１７であった場合（Ｓ２１５；ＹＥＳ）には、ステップＳ２１６へ処理を進める。

【０１１２】

ステップＳ２１６では、監視処理プロセス４１ａは、ステップＳ２１１において受信したパケットのＩＣＭＰオプションフィールドから、その時間超過メッセージを生成する基となったパケットがレイヤ４ヘッダの送信先ポート番号フィールドに持っていた送信先ポート番号を読み取る。読み取り後、監視処理プロセス４１ａは、ステップＳ２１７へ処理を進める。

【０１１３】

ステップＳ２１７では、監視処理プロセス４１ａは、調査処理プロセスを実行する。つまり、第２のルーティングループ検出装置４０には、調査処理プロセスが生成される。なお、調査処理プロセスは、この監視処理プロセス４１ａと並行に実行される。また、調査処理プロセスの内容については、図１２乃至図１４を用いて後述する。この調査処理プロセスの生成後、監視処理プロセス４１ａは、ステップＳ２１８へ処理を進める。

【０１１４】

ステップＳ２１８では、監視処理プロセス４１ａは、ステップＳ２１３，Ｓ２１４において読み取ったＩＰアドレス及びプロトコル番号と、ステップＳ２１５，Ｓ２１６において読み取れた場合には更にポート番号とを、調査対象情報として、調査処理プロセスへ引き渡す。その後、監視処理プロセス４１ａは、ステップＳ２１９へ処理を進める。

【０１１５】
ステップＳ２１９では、監視処理プロセス４１ａは、調査処理プロセスが消滅したか否かを、判別する。そして、調査処理プロセスが消滅していなかった場合（Ｓ２１９；ＮＯ）には、監視処理プロセス４１ａは、ステップＳ２２０へ処理を進める。
【０１１６】
ステップＳ２２０では、監視処理プロセス４１ａは、調査処理プロセスから、後述の通知があったか否かを、判別する。そして、後述の通知が調査処理プロセスからなかった場合（Ｓ２２０；ＮＯ）には、監視処理プロセス４１ａは、ステップＳ２１９へ処理を戻す。
【０１１７】
ステップＳ２１９，Ｓ２２０の処理ループの実行中、後述の通知が調査処理プロセスからある前に、調査処理プロセスが消滅した場合（Ｓ２１９；ＹＥＳ）には、監視処理プロセス４１ａは、ステップＳ２１１へ処理を戻す。一方、この処理ループの実行中、調査処理プロセスが消滅する前に、後述の通知が調査処理プロセスからあった場合（Ｓ２２０；ＹＥＳ）には、監視処理プロセス４１ａは、監視処理を終了する。
【０１１８】
図１２及び図１３は、調査処理の内容を説明するためのフローチャートである。調査処理の開始後、最初のステップＳ２２１では、ＣＰＵ４０ａ（以下、ＣＰＵ４０ａが調査プログラム４１ｂを実行することによって実現される機能を、調査処理プロセス４１ｂと表記する）は、調査対象情報が監視処理プロセス４１ａから引き渡されるまで、待機する（Ｓ２２１；ＮＯ）。そして、調査対象情報を監視処理プロセス４１ａから受け取ると（Ｓ２２１；ＹＥＳ）、調査処理プロセス４１ｂは、ステップＳ２２２へ処理を進める。
【０１１９】
ステップＳ２２２では、調査処理プロセス４１ｂは、監視処理プロセス４１ａから引き渡された調査対象情報により示される宛先が、調査すべき対象であるか否かを、判別する。
【０１２０】
なお、調査しなくても良い対象は、ＨＤＤ４０ｄ内に事前に用意されるフィルタリングテーブルにより、管理される。フィルタリングテーブルには、調査しなくて良い対象を選別するための条件としてネットワークＮの管理者にて選択されたＩＰアドレス，プロトコル番号，及び、ポート番号が、登録されている。
【０１２１】
そして、ステップＳ２２２において、調査処理プロセス４１ｂは、調査対象情報中のＩＰアドレス及びプロトコル番号（存在する場合にはポート番号も）の何れかに一致するものがフィルタリングテーブルに登録されていた場合（Ｓ２２２；ＮＯ）には、この調査対象情報により示される宛先が調査すべき対象でないとして、調査処理を終了する。
【０１２２】
一方、ステップＳ２２２において、調査処理プロセス４１ｂは、調査対象情報中のＩＰアドレス及びプロトコル番号（存在する場合にはポート番号も）の何れもがフィルタリングテーブルに登録されているものと一致しなかった場合（Ｓ２２２；ＹＥＳ）には、この調査対象情報により示される宛先が調査すべき対象であるとして、ステップＳ２２３へ処理を進める。
【０１２３】
ステップＳ２２３では、調査処理プロセス４１ｂは、調査対象情報中のＩＰアドレスが調査を待機すべき対象であるか否かを、判別する。
【０１２４】
なお、調査を待機すべき対象は、ＲＡＭ４０ｂ内の待機対象管理テーブルにより、管理される。待機対象管理テーブルには、一旦調査対象とされて調査がなされたＩＰアドレスを含むサブネットのネットワークアドレスであって、その調査から所定待機期間が経過してないものが、登録されている。より具体的には、待機対象管理テーブルには、ネットワ

ークアドレスと待機開始時刻とからなるレコードが、蓄積されている。

【０１２５】

そして、ステップＳ２２３において、調査処理プロセス４１ｂは、調査対象情報中のＩＰアドレスを含むサブネットのネットワークアドレスが待機対象管理テーブルに登録されていなかった場合（Ｓ２２３；ＮＯ）には、当該ＩＰアドレスが調査を即時に開始すべき対象であるとして、ステップＳ２２４へ処理を進める。

【０１２６】

ステップＳ２２４では、調査処理プロセス４１ｂは、当該ＩＰアドレスを含むサブネットのネットワークアドレスと、待機開始時刻としての現在時刻とからなるレコードを、ＲＡＭ４０ｂ内の待機対象管理テーブルに登録する。登録後、調査処理プロセス４１ｂは、ステップＳ２２７へ処理を進める。

【０１２７】

一方、ステップＳ２２３において、調査処理プロセス４１ｂは、調査対象情報中のＩＰアドレスを含むサブネットのネットワークアドレスが待機対象管理テーブルに登録されていた場合（Ｓ２２３；ＹＥＳ）には、当該ＩＰアドレスが調査を待機すべき対象であるとして、ステップＳ２２５へ処理を進める。

【０１２８】

ステップＳ２２５では、調査処理プロセス４１ｂは、当該ＩＰアドレスを含むサブネットのネットワークアドレスに対応する待機開始時刻から、事前に設定された待機期間（例えば１０分）が経過しているか否かを、判別する。そして、調査処理プロセス４１ｂは、当該待機開始時刻から待機期間が経過していなかった場合（Ｓ２２５；ＮＯ）には、調査処理を終了し、当該待機開始時刻から待機期間が経過していた場合（Ｓ２２５；ＹＥＳ）には、ステップＳ２２６へ処理を進める。

【０１２９】

ステップＳ２２６では、調査処理プロセス４１ｂは、調査対象のＩＰアドレスを含むサブネットのネットワークアドレスのレコードを待機対象管理テーブルから削除する。削除後、調査処理プロセス４１ｂは、ステップＳ２２７へ処理を進める。

【０１３０】

ステップＳ２２７では、調査処理プロセス４１ｂは、調査対象情報に対応する一部作成済パケットを、ＨＤＤ４０ｄから読み出す。

【０１３１】

ここで、一部作成済パケットとは、何れの宛先を調査対象とした場合でも不変である情報が各ヘッダの所定のフィールドに予め組み込まれているパケットをいう。この一部作成済パケットは、調査対象に応じて内容を書き換えねばならないフィールドの内容のみを、調査時に書き換えるだけで済ませるためのものである。すなわち、このような一部作成済パケットがＨＤＤ４０ｄに事前に格納されていると、図２のパケット送信プログラム３３と同等のプログラムに調査用パケットを作成させなくとも、ＨＤＤ４０ｄから読み出して所定のフィールドの内容を書き換えるだけで、調査用パケットを即時に完成させることができる。

【０１３２】

なお、本実施形態では、この一部作成済パケットは、プロトコル番号毎に用意されている。つまり、ＨＤＤ４０ｄには、ＩＰヘッダのプロトコル番号フィールドの内容が互いに異なる一部作成済パケットが、プロトコル番号の数だけ用意されている。但し、一部作成済パケットは、一種類だけ用意されていても良い。何れの場合でも、一部作成済パケットの残存ホップ数は、最大値の２５５に設定されている。

【０１３３】

前者のようにプロトコル番号の数だけ用意されている場合、ＩＰバージョン４においては、ＩＰヘッダ中の識別番号フィールド，ヘッダチェックサムフィールド，及び、送信先ＩＰアドレスフィールドが、調査対象に応じて書き換えねばならないフィールドとなり、ＩＰバージョン６においては、ＩＰヘッダ中の送信先ＩＰアドレスフィールドが、調査対

象に応じて書き換えねばならないフィールドとなる。

【０１３４】

一方、後者のように一部作成済パケットが一種類だけ用意されている場合には、ＩＰバージョン４においては、ＩＰヘッダ中のプロトコル番号フィールドが、更に、調査対象に応じて書き換えねばならないフィールドとして追加され、ＩＰバージョン６においては、ＩＰヘッダ中のネクストヘッダフィールドが、更に、調査対象に応じて書き換えねばならないフィールドとして追加される。

【０１３５】

また、ＨＤＤ４０ｄに事前に用意される複数の一部作成済パケットには、何れも、プロトコル番号に応じたレイヤ３ヘッダ（ＩＰヘッダを除く）又はレイヤ４ヘッダが、含まれることとなるが、特に、プロトコル番号が６又は１７である一部作成済パケットには、ＴＣＰヘッダ又はＵＤＰヘッダのレイヤ４ヘッダが、含まれることとなる。そして、このレイヤ４ヘッダを持つ二つの一部作成済パケットにおいては、さらに、送信先ポート番号フィールド及びチェックサムフィールドが、調査対象に応じて書き換えねばならないフィールドとなる。

【０１３６】

ステップＳ２２７では、調査処理プロセス４１ｂは、調査対象情報中のプロトコル番号（存在する場合にはポート番号も）に対応する一部作成済パケットを、ＨＤＤ４０ｄから読み出し、ステップＳ２２８へ処理を進める。

【０１３７】

ステップＳ２２８では、調査処理プロセス４１ｂは、ＨＤＤ４０ｄから読み出した一部作成済パケットにおける所定のフィールドの内容を書き換えることにより、調査用パケットを生成する。生成後、調査処理プロセス４１ｂは、ステップＳ２２９へ処理を進める。

【０１３８】

ステップＳ２２９では、調査処理プロセス４１ｂは、ステップＳ２２８において生成した調査用パケットを、通信制御装置４０ｃへ引き渡すことによって、調査対象情報中のＩＰアドレス宛へ送信する。送信後、調査処理プロセス４１ｂは、ステップＳ２３０へ処理を進める。

【０１３９】

ステップＳ２３０では、調査処理プロセス４１ｂは、調査用パケットの応答としてのパケットを受信するまで、待機する（Ｓ２３０；ＮＯ）。なお、この受信には、パケット受信プログラム４３による機能が用いられる。そして、調査用パケットの応答としてのパケットを受信すると（Ｓ２３０；ＹＥＳ）、調査処理プロセス４１ｂは、ステップＳ２３１へ処理を進める。

【０１４０】

ステップＳ２３１では、調査処理プロセス４１ｂは、調査用パケットの応答として受信したパケットが時間超過メッセージ付きパケットであるか否かを、判別する。そして、調査処理プロセス４１ｂは、受信したパケットが時間超過メッセージ付きパケットでなかった場合（Ｓ２３１；ＮＯ）には、調査処理を終了し、受信したパケットが時間超過メッセージ付きパケットであった場合（Ｓ２３１；ＹＥＳ）には、ステップＳ２３２へ処理を進める。

【０１４１】

ステップＳ２３２では、調査処理プロセス４１ｂは、調査用パケットの応答として受信したパケットの送信元のＩＰアドレスが兆候通知中のＩＰアドレスと同じであるか否かを、判別する。そして、調査処理プロセス４１ｂは、調査用パケットの応答として受信したパケットの送信元のＩＰアドレスが兆候通知中のＩＰアドレスと同じでなかった場合（Ｓ２３２；ＮＯ）には、調査処理を終了し、調査用パケットの応答として受信したパケットの送信元のＩＰアドレスが兆候通知中のＩＰアドレスと同じであった場合（Ｓ２３２；ＹＥＳ）には、ステップＳ２３３へ処理を進める。

【０１４２】

ステップＳ２３３では、調査処理プロセス４１ｂは、ループ位置特定処理サブルーチンを実行する。図１３及び図１４は、ループ位置特定処理サブルーチンの内容を説明するためのフローチャートである。

【０１４３】

ループ位置特定処理サブルーチンの開始後、最初のステップＳ２５１では、調査処理プロセス４１ｂは、ＲＡＭ４０ｂ内のワークテーブルを初期化するとともに、変数Ｘの値をゼロにする。なお、ワークテーブルは、ＩＰアドレスを格納するためのものである。調査処理プロセス４１ｂは、ワークテーブル内の全てのレコードを削除することによって、ワークテーブルを初期化する。その後、調査処理プロセス４１ｂは、ステップＳ２５２へ処理を進める。

【０１４４】

ステップＳ２５２では、調査処理プロセス４１ｂは、変数Ｘの代入値を１だけインクリメントする。インクリメント後、調査処理プロセス４１ｂは、ステップＳ２５３へ処理を進める。

【０１４５】

ステップＳ２５３では、調査処理プロセス４１ｂは、変数Ｘの代入値が２５５であるか否かを、判別する。そして、変数Ｘの代入値が２５５でなかった場合（Ｓ２５３；ＮＯ）には、調査処理プロセス４１ｂは、ステップＳ２５４へ処理を進める。

【０１４６】

ステップＳ２５４では、調査処理プロセス４１ｂは、ＩＰヘッダの生存時間（又はホップリミット）フィールドに変数Ｘの代入値を持つとともに、エコー要求メッセージを持つパケットを生成する。なお、エコー要求メッセージとは、タイプフィールドに８を持つＩＣＭＰヘッダのことである。パケット生成後、調査処理プロセス４１ｂは、ステップＳ２５５へ処理を進める。

【０１４７】

ステップＳ２５５では、調査処理プロセス４１ｂは、ステップＳ２３０において受信したパケットの送信元のノードのＩＰアドレス宛へ当該パケットを送信し、ステップＳ２５６へ処理を進める。

【０１４８】

ステップＳ２５６では、調査処理プロセス４１ｂは、ステップＳ２５５において送信したパケットの応答としてのパケットを受信するまで、待機する（Ｓ２５６；ＮＯ）。なお、この受信には、パケット受信プログラム４３による機能が用いられる。そして、応答としてのパケットを受信すると（Ｓ２５６；ＹＥＳ）、調査処理プロセス４１ｂは、ステップＳ２５７へ処理を進める。

【０１４９】

ステップＳ２５７では、調査処理プロセス４１ｂは、受信したパケットがエコー応答メッセージ付きパケットであるか否かを、判別する。すなわち、タイプフィールドに０を持つＩＣＭＰヘッダは、エコー応答メッセージと称されているが、調査処理ステップ４１は、ステップＳ２５７において、受信したパケットにおけるＩＰヘッダを除く部分にこのエコー応答メッセージが含まれているか否かを、判別する。そして、受信したパケットがエコー要求メッセージ付きパケットでなかった場合（Ｓ２５７；ＮＯ）には、調査処理ステップ４１ａは、受信したパケットが時間超過メッセージを含むものであるとして、ステップＳ２５８へ処理を進める。

【０１５０】

ステップＳ２５８では、調査処理プロセス４１ｂは、時間超過メッセージ付きパケットを送信してきたノードのＩＰアドレスがＲＡＭ４０ｂ内のワークテーブルに登録済であるか否かを、判別する。具体的には、調査処理プロセス４１ｂは、時間超過メッセージ付きパケットのＩＰヘッダの送信元ＩＰアドレスフィールドからＩＰアドレスを読み取り、この読み取ったＩＰアドレスにてワークテーブル内を検索し、そのＩＰアドレスと同じＩＰアドレスがワークテーブルから検出できるか否かを、判別する。そして、時間超過メッセ

ージ付きのパケットを送信してきたノードのＩＰアドレスがＲＡＭ４０ｂ内のワークテーブルに登録されていなかった場合（Ｓ２５８；ＮＯ）には、調査処理プロセス４１ｂは、ステップＳ２５９へ処理を進める。

【０１５１】

ステップＳ２５９では、調査処理プロセス４１ｂは、時間超過メッセージ付きパケットを送信してきたノードのＩＰアドレスをワークテーブルに登録する。具体的には、調査処理プロセス４１ｂは、時間超過メッセージ付きパケットのＩＰヘッダの送信元ＩＰアドレスフィールドからＩＰアドレスを読み取り、この読み取ったＩＰアドレスを変数Ｘの代入値とともにワークテーブルに記録する。記録後、調査処理プロセス４１ｂは、ステップＳ２５２へ処理を戻す。

【０１５２】

ステップＳ２５２～Ｓ２５９の処理ループの実行中、変数Ｘの代入値が２５５に達してしまった場合には、調査処理プロセス４１ｂは、ステップＳ２５３からステップＳ２６０へ処理を分岐させる（Ｓ２５３；ＹＥＳ）。

【０１５３】

ステップＳ２６０では、調査処理プロセス４１ｂは、ルーティングループを発生させているルータの特定に失敗した旨を、監視処理プロセス４１ａに通知する。通知後、調査処理プロセス４１ｂは、図１４のループ位置特定処理サブルーチンを終了するとともに、図１２及び図１３の調査処理を終了する。

【０１５４】

また、ステップＳ２５２～Ｓ２５９の処理ループの実行中、変数Ｘの代入値が２５５に達してしまう前に、エコー要求メッセージ付きパケットの応答としてエコー応答メッセージ付きパケットを受信した場合には、調査処理プロセス４１ｂは、ステップＳ２５７からステップＳ２６１へ処理を分岐させる（Ｓ２５７；ＹＥＳ）。

【０１５５】

ステップＳ２６１では、調査処理プロセス４１ｂは、ルーティングループが解消された旨を、監視処理プロセス４１ａに通知する。通知後、調査処理プロセス４１ｂは、図１４のループ位置特定処理サブルーチンを終了するとともに、図１２及び図１３の調査処理を終了する。

【０１５６】

また、ステップＳ２５２～Ｓ２５９の処理ループの実行中、変数Ｘの代入値が２５５に達してしまう前に、ＩＰアドレスがワークテーブルに一旦登録されたノードから再び時間超過メッセージ付きパケットを受信した場合には、調査処理プロセス４１ｂは、ステップＳ２５８からステップＳ２６２へ処理を分岐させる（Ｓ２５８；ＹＥＳ）。

【０１５７】

ステップＳ２６２では、調査処理プロセス４１ｂは、ワークテーブルにおいて、時間超過メッセージ付きパケットを再び送信してきたノードのＩＰアドレスを特定し、このＩＰアドレスからＸ－１番目のＩＰアドレスまでの各ＩＰアドレスを、ワークテーブルから読み出す。読み出し後、調査処理プロセス４１ｂは、ステップＳ２６３へ処理を進める。

【０１５８】

ステップＳ２６３では、調査処理プロセス４１ｂは、ステップＳ２６２において読み出したＩＰアドレスとともに、ルーティングループを発生させているルータの特定に成功した旨を、監視処理プロセス４１ａに通知する。通知後、調査処理プロセス４１ｂは、図１４のループ位置特定処理サブルーチンを終了するとともに、図１２及び図１３の調査処理を終了する。

【０１５９】

このように、調査処理プロセス４１ｂは、ステップＳ２６０，Ｓ２６１，Ｓ２６３の何れかを実行することにより、監視処理プロセス４１ａへ、ループ位置特定処理の結果である何らかの通知を行うこととなる。なお、上述したように、この監視処理プロセス４１ａは、調査処理プロセス４１ｂが消滅する前に、調査処理プロセス４１ｂから何れかの通知

を受けると、監視処理を終了する（Ｓ２２０；ＹＥＳ）。但し、調査処理プロセス４１ｂは、ループ位置特定処理サブルーチンを実行せず（つまり何れかの通知をすることなく）に終了することもあり（Ｓ２２２；ＮＯ，Ｓ２２５；ＮＯ，Ｓ２３１；ＮＯ）、この場合（Ｓ２１９；ＮＯ）、監視処理プロセス４１ａは、再び、時間超過メッセージ付きパケットがキャプチャされるのを監視し（Ｓ２１１，Ｓ２１２）、何個目かの調査処理プロセスから通知があるまで監視処理を継続する。

【０１６０】

一方、図１０の第２のルーティングループ検出処理では、ＣＰＵ４０ａは、ステップＳ２０１において監視処理プロセスを生成した後、ステップＳ２０２において、監視処理プロセス４１ａが消滅するのを、監視している（Ｓ２０２；ＮＯ）。そして、監視処理プロセス４１ａが何個目かの調査処理プロセス４１ｂからの通知を受けて消滅すると（Ｓ２０２；ＹＥＳ）、ＣＰＵ４０ａは、ステップＳ２０３へ処理を進める。

【０１６１】

ステップＳ２０３では、ＣＰＵ４０ａは、ルーティングループを発生させているルータの特定に失敗した旨が調査処理ステップ４１ｂから監視処理プロセス４１ａへ通知されたか否かを、判別する。そして、特定失敗の旨が調査処理ステップ４１ｂから監視処理プロセス４１ａへ通知されていた場合（Ｓ２０３；ＹＥＳ）には、ＣＰＵ４０ａは、ステップＳ２０４へ処理を進める。

【０１６２】

ステップＳ２０４では、ＣＰＵ４０ａは、ルーティングループを発生させているルータの特定に失敗した旨とともに、兆候通知に含まれるＩＰアドレスにより示されるルータにおいてルーティングループが発生した虞がある旨を、出力する。なお、出力方法としては、例えば、それらの旨を記述した画面をディスプレイ等に表示したり、その旨を記述した電子メールをネットワークＮの管理者のパーソナルコンピュータへ送信したりすることができる。出力後、ＣＰＵ４０ａは、第２のルーティングループ検出処理を終了する。

【０１６３】

一方、ステップＳ２０３において、ルーティングループを発生させているルータの特定に失敗した旨が調査処理ステップ４１ｂから監視処理プロセス４１ａへ通知されていなかった場合（Ｓ２０３；ＮＯ）には、ＣＰＵ４０ａは、ステップＳ２０５へ処理を進める。

【０１６４】

ステップＳ２０５では、ＣＰＵ４０ａは、ルーティングループが解消された旨が調査処理ステップ４１ｂから監視処理プロセス４１ａへ通知されたか否かを、判別する。そして、ルーティングループが解消された旨が調査処理ステップ４１ｂから監視処理プロセス４１ａへ通知されていた場合（Ｓ２０５；ＹＥＳ）には、ＣＰＵ４０ａは、ステップＳ２０６へ処理を進める。

【０１６５】

ステップＳ２０６では、ＣＰＵ４０ａは、兆候通知に含まれるＩＰアドレスにより示されるルータにおいてルーティングループが発生した虞がある旨を、出力する。なお、出力方法としては、上述したのと同様に、ディスプレイ表示や、電子メール送信などとすることができる。出力後、ＣＰＵ４０ａは、第２のルーティングループ検出処理を終了する。

【０１６６】

一方、ステップＳ２０５において、ルーティングループが解消された旨が調査処理ステップ４１ｂから監視処理プロセス４１ａへ通知されていなかった場合（Ｓ２０３；ＮＯ）には、ＣＰＵ４０ａは、ルーティングループを発生させているルータの特定に成功した旨が監視処理プロセス４１ａに通知されたとして、ステップＳ２０７へ処理を進める。

【０１６７】

ステップＳ２０７では、ＣＰＵ４０ａは、ルーティングループが発生している旨と、ルーティングループの発生箇所が特定できた旨とを、出力するとともに、その発生箇所を示す情報として、監視処理プロセス４１ａに通知されたＩＰアドレスを、出力する。なお、出力方法としては、上述したのと同様に、ディスプレイ表示や、電子メール送信などとす

ることができる。出力後、ＣＰＵ４０ａは、第２のルーティングループ検出処理を終了する。

【０１６８】

以上に説明した第２のルーティングループ検出処理が実行されることにより、第２のルーティングループ検出装置４０は、以下に説明するように作用する。

【０１６９】

第２のルーティングループ検出装置４０は、何れかの第１のルーティングループ検出装置３０からの兆候通知を受けると、監視処理プロセス４１を生成することによって、ネットワークＮの内部から外部へ流れていく時間超過メッセージ付きパケットを監視する処理を、開始する（Ｓ２０１，Ｓ２１１，Ｓ２１２）。そして、第２のルーティングループ検出装置４０は、時間超過メッセージ付きパケットをキャプチャすると（Ｓ２１２；ＹＥＳ）、ゲートウエイルータ１０’から、その時間超過メッセージを生成する基となったパケットの送信先までの経路を、調査対象として特定するため、その送信先に関する情報（送信先ＩＰアドレス，プロトコル番号，送信先ポート番号）を時間超過メッセージから読み取り（Ｓ２１３～Ｓ２１６）、調査処理プロセス４１ｂを生成することによって、調査を開始する（Ｓ２１７，Ｓ２１８，Ｓ２２１）。

【０１７０】

そして、第２のルーティングループ検出装置４０は、その対象が調査すべき対象であって、且つ、調査を待機すべきでない対象であったときに（Ｓ２２２；ＹＥＳ，Ｓ２２５；ＹＥＳ）、その調査対象に向けて調査用パケットを送信して、応答を待つ（Ｓ２２６～Ｓ２３０）。

【０１７１】

その応答として時間超過メッセージ付きでないパケットを受信すると、監視処理を再開する（Ｓ２３１；ＮＯ，Ｓ２１９；ＹＥＳ，Ｓ２１１，Ｓ２１２）が、その応答として時間超過メッセージ付きパケットを受信すると（Ｓ２３１；ＹＥＳ）、第２のルーティングループ検出装置４０は、そのパケットの送信元が第１のルーティングループ検出装置３０から通知されたＩＰアドレスと同じであるか判別し（Ｓ２３２）、同じであった場合には、調査対象となる経路においてルーティングループが発生しているとして、そのルーティングループを発生させているルータの特定に取り掛かる（Ｓ２３３）。

【０１７２】

このルータの特定に用いられているループ位置特定処理サブルーチン（Ｓ２５１～Ｓ２６３）には、いわゆるトレースルートの手法が用いられている。すなわち、第２のルーティングループ検出装置４０は、残存ホップ数が互いに異なるエコー要求メッセージ付きパケットを順次調査対象に送信し（Ｓ２５２～Ｓ２５６）、その応答として時間超過メッセージ付きパケットを受信して、そのパケットの送信元ノードのＩＰアドレスを記録する（Ｓ２５９）。そして、第２のルーティングループ検出装置４０は、エコー応答メッセージ付きパケットが送られてくる前であって、且つ、残存ホップ数が最大値の２５５に達する前に、同一ノードから時間超過メッセージ付きパケットが繰り返し送られてくるようになってきたときに、記録しておいたＩＰアドレスの中から、ルーティングループを発生させているルータのＩＰアドレスを特定する（Ｓ２６２）。

【０１７３】

第２のルーティングループ検出装置４０は、このトレースルートの手法により、ルーティングループを発生させているルータのＩＰアドレスが特定できたときには（Ｓ２５８；ＹＥＳ）、ルーティングループを発生させているルータを特定できた旨を出力する（Ｓ２６２，Ｓ２６３，Ｓ２０５；ＹＥＳ，２０７）。

【０１７４】

このように作用するために、第２のルーティングループ検出装置４０は、以下に説明するような効果を奏する。

【０１７５】

すなわち、従来の方法（上述した第３の方法）によれば、監視対象となるパケット全て

について同一内容か否かを一つ一つ検査する必要があった。この検査に必要な１パケット当たりのデータ量は、上述したように、ＩＰバージョン４においては、１３バイトであり、ＩＰバージョン６においては、３６バイトである。しかし、本実施形態の第２のルーティングループ検出装置３０は、全パケットを監視することにはなるとしても、ＩＰヘッダのプロトコル番号フィールド(１バイト)が１であるかどうか、プロトコル番号が１である場合にはＩＣＭＰヘッダのタイプフィールド(１バイト)が１１であるかどうかという簡易な処理を行うだけである。然も、全パケットにおける全ての組み合わせについて互いにマッチングするか否かを判別するというような重い処理も行わない。そのうえ、第２のルーティングループ検出装置４０は、ゲートウエイルータ１０’から外部に流出しようとするパケットの中から、時間超過メッセージ付きパケットのみを検出し、ゲートウエイルータ１０’に流れ込む全てのパケットについて処理を行うわけではない。このため、パケットの流入量が非常に膨大であっても、パケットキャプチャ時に、第２のルーティングループ検出装置４０には、処理負荷が殆ど掛からない。つまり、第２のルーティングループ検出装置４０は、ゲートウエイルータ１０’の下流側の通信回線の通信速度が非常に高速であったとしても、すなわち、大規模なネットワークに適用されたとしても、適切に処理を行える。

【０１７６】

なお、時間超過メッセージ付きパケットは、パケットが消滅したときに生成されるものであるが、このようなパケットの消滅は、ルーティングループ以外にも、例えば、トレースルートやアタックによっても引き起こされ得る。つまり、ルーティングループが発生してパケットが消滅したときには、時間超過メッセージ付きパケットが必ず送られてくるものの、時間超過メッセージ付きパケットが必ずルーティングループの発生を示している訳ではない。従って、第２のルーティングループ検出装置４０は、時間超過メッセージ付きパケットを監視することによって、少なくとも、ルーティングループの発生の兆候を見逃さないと言うことができる。

【０１７７】

そこで、この第２のルーティングループ検出装置４０は、時間超過メッセージ付きパケットをキャプチャしたときには、本来の送信先へ調査用パケットを送信する。ここで、再度、時間超過メッセージ付きパケットが返ってきたときには、この時間超過メッセージ付きパケットは、トレースルートやアタック等に因るものではなく、ルーティングループに因るものであると言える。このため、第２のルーティングループ検出装置４０は、時間超過メッセージ付きパケットのキャプチャ後、本来の送信先へ調査用パケットを送信するだけで、ネットワークＮ内においてルーティングループが生じているか否かを、確実に検出することができる。

【０１７８】

また、第２のルーティングループ検出装置４０は、時間超過メッセージ付きパケットのキャプチャ後、本来の送信先へ即座に調査用パケットを送信する。また、その応答も数秒と掛からずに返ってくる。従って、第２のルーティングループ検出装置４０によれば、ネットワークＮ内においてルーティングループが生じたか否かを、即座に確認することができる。

【０１７９】

また、調査用パケットの応答として時間超過メッセージ付きパケットを受けただけでは、ネットワークＮ内にルーティングループが発生していることしか確認できないが、第２のルーティングループ検出装置４０は、調査用パケットの応答としての時間超過メッセージ付きパケットを受信したときには、トレースルートの手法を用いて、ルーティングループを発生させているルータの特定に掛かる。これにより、ネットワークＮ内で発生したルーティングループの発生位置をできるだけ特定することができるようになる。

【０１８０】

また、第２のルーティングループ検出装置４０では、フィルタリングテーブルに何も定義しておかなければ、時間超過メッセージ付きパケットのキャプチャ後、本来の送信先へ

調査用パケットを必ず送信することとなるが、フィルタリングテーブルに所定の情報を登録しておけば、その条件に合致した送信先へは、調査用パケットが送られることがない。なお、このフィルタリングテーブルに登録する条件としては、例えば、調査の必要が無いノードのＩＰアドレス，既にルーティングループが検出されて復旧作業が行われているノードのＩＰアドレス，本来の送信先において動作していることが有り得ないポート番号などがある。このように、フィルタリングテーブルを用いて、調査用パケットの送り先を制限することにより、ネットワークＮに余計な負荷を与えたり、アタックと看做されるようなパケットをネットワークＮに送らなくて済む。

【０１８１】

また、ゲートウエイルータ１０’直前を流れる時間超過メッセージ付きパケットは、トレースルートやアタックに因って短期間に大量に発生し、さらには、例えば１つのテキストデータから小分けされた一連のパケットが一つの送信先に送られてそれらが全て同様のルーティングループに陥ってしまうことによっても短期間に大量に発生する。このように短期間に大量に発生した時間超過メッセージ付きパケットに基づく調査対象は、ほぼ同一のものである可能性が高く、大量に発生する時間超過メッセージ付きパケットの全てについていちいち調査用パケットを送信していたのでは、ネットワークＮに負荷を掛けてしまう虞が高い。そこで、第２のルーティングループ検出装置４０では、一旦調査用パケットが送られた送信先のＩＰアドレスを含むサブネットのネットワークアドレスを、待機対象管理テーブルに登録することにより、一旦調査されたサブネットに対して、一定期間調査用パケットを送られないようにしている。こうすることで、調査回数を大幅に減らすことができ、その結果、ネットワークＮへの負荷を軽減することができる。

【０１８２】

また、第２のルーティングループ検出装置４０では、一部作成済パケットがＨＤＤ４０ｄに事前に格納されている。これにより、時間超過メッセージ付きパケットのキャプチャ後、ＨＤＤ４０ｄから読み出した一部作成済パケットの一部を書き換えれば、即座に調査用パケットを生成することができ、時間超過メッセージ付きパケットをキャプチャする毎にいちいち調査用パケットを新規に生成しなくても済む。その結果、処理速度の低減を防止することができることとなる。

【０１８３】

また、調査用パケットの送信先やその途中のノードにおいて、セキュリティのために、パケットがＩＰヘッダ以外に持つデータ（レイヤ４ヘッダ又はレイヤ３ヘッダ）に応じてその通過が制限されていることがある（いわゆるパケットフィルタリング）。この場合、調査用パケットを送信しても、その調査用パケットが途中で破棄されてしまい、適正な応答が返ってこないことがある。これに対し、この第２のルーティングループ検出装置４０は、ゲートウエイルータ１０’に流れ込む時間超過メッセージ付きパケットから、その本来の送信先のＩＰアドレスの他に、プロトコル番号やポート番号を読み取り、そのプロトコル番号やポート番号に対応するデータ（レイヤ４ヘッダ又はレイヤ３ヘッダ）をＩＰヘッダに付加することにより、送信先において動作している通信サービス（例えば、echo, daytime, telnet, FTP [File Transfer Protocol] , ssh [Secure Shell] , http [Hyper Text Transfer Protocol] , POP [Post Office Protocol] , SMTP [Simple Mail Transfar Protocol] , DNS [Domain Name Server] ）が要求するパケットを生成する。これにより、調査用パケットを送るためのポート等を開けるような作業を本来の送信先に対して行わなくても、パケットフィルタリングによる通過禁止を避ることができ、また、その結果として、その送信先のセキュリティレベルを一時的に低下させることもない。

【０１８４】

なお、上述した本実施形態では、調査用パケットにおけるＩＰヘッダに付加されるデータは、本来の送信先についてのプロトコル番号やポート番号に対応するデータ（レイヤ４ヘッダ又はレイヤ３ヘッダ）であったが、これに限られるものではない。この調査用パケットがエコー要求メッセージを含むものである場合を、その変形例として、以下に示す。

【０１８５】

＜変形例＞

図１５は、本実施形態の変形例での監視処理を説明するためのフローチャートである。この図１５と図１１とを比較して明らかなように、変形例における監視処理は、図１１のステップＳ２１４～Ｓ２１６を省略したものとなっている。

【０１８６】

すなわち、監視処理プロセス４１ａは、パケットキャプチャプログラム４２から受け取ったパケットが時間超過メッセージ付きパケットであった場合（Ｓ３１２）、ステップＳ３１１において受信した時間超過メッセージ付きパケットのＩＣＭＰヘッダのＩＣＭＰオプションフィールドから、このパケットを発生させる基となったパケットの送信先のＩＰアドレスを読み取り（Ｓ３１３）、その後、直ぐに、調査処理プロセスの生成に取り掛かる（Ｓ３１７）。

【０１８７】

従って、この変形例においては、監視処理プロセス４１ａから調査処理プロセス４１ｂへ引き渡される調査対象情報には、本来の送信先のＩＰアドレスだけが含まれることとなる。

【０１８８】

一方、変形例における調査処理プロセス４１ｂは、調査対象が待機対象でなかった場合（Ｓ２２５；ＹＥＳ）には、エコー要求メッセージが含まれるように構成された一部作成済パケットをＨＤＤ４０ｄから読み出す（Ｓ２２７）。すなわち、変形例における一部作成済パケットは、残存ホップ数として最大値の２５５を持つＩＰヘッダと、タイプフィールドに８を持つＩＣＭＰヘッダとからなっている。調査処理プロセス４１ｂは、このように構成される一部作成済パケットをＨＤＤ４０ｄから読み出した後、所定のフィールドを変更し（Ｓ２２８）、調査対象となる宛先へこの調査用パケットを送信し（Ｓ２２９）、その応答を待つ（Ｓ２３０）。

【０１８９】

このとき、この調査用パケットの応答として送られてくるパケットは、エコー応答メッセージ付きパケットか、時間超過メッセージ付きパケットとなるが、ルーティングループが発生していることにより送られてくるパケットは、上述した変形前の実施形態と同様に、時間超過メッセージ付きパケットとなる。従って、変形例による第２のルーティングループ検出装置４０も、上述した変形前の実施形態と同様の効果を奏することとなる。

読み取り後、監視処理プロセス４１は、ステップＳ２１４へ処理を進める。

【０１９０】

（付記１）

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出手段，

前記パケット抽出手段が抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先ＩＰアドレスを読み取る読取手段，

前記読取手段が読み取った送信先ＩＰアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信手段，

前記パケット送信手段が送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信手段，及び、

前記パケット受信手段が受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティングループが発生している旨を出力する出力手段

として機能させる

ことを特徴とするルーティングループ検出プログラム。

【０１９１】

（付記２）

前記調査用パケットは、アプリケーション層上に存在するネットワークアプリケーションサービスについてのサービス要求パケットである

ことを特徴とする付記１記載のルーティングループ検出プログラム。

【０１９２】

（付記３）

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をＩＰヘッダ中に有するパケットの個数を、計数する計数手段，

前記計数手段が計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別手段，及び、

前記判別手段が前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティングループの発生の兆候がある旨を出力する出力手段

として機能させる

ことを特徴とするルーティングループ検出プログラム。

【０１９３】

（付記４）

コンピュータが、

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出ステップと、

前記パケット抽出ステップにおいて抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先ＩＰアドレスを読み取る読取ステップと、

前記読取ステップにおいて読み取った送信先ＩＰアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信ステップと、

前記パケット送信ステップにおいて送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信ステップと、

前記パケット受信ステップにおいて受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティングループが発生している旨を出力する出力ステップと

を実行する

ことを特徴とするルーティングループ検出方法。

【０１９４】

（付記５）

コンピュータが、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をＩＰヘッダ中に有するパケットの個数を、計数する計数ステップと、

前記計数ステップにおいて計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別ステップと、

前記判別ステップにおいて前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティングループの発生の兆候がある旨を出力する出力ステップと

を実行する

ことを特徴とするルーティングループ検出方法。

【０１９５】

（付記６）

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出部と、

前記パケット抽出部において抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先ＩＰアドレスを読み取る読取部と、

前記読取ステップ部において読み取った送信先ＩＰアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信部と、

前記パケット送信部において送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信部と、

前記パケット受信部において受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティングループが発生している旨を出力する出力部と
を備えることを特徴とするルーティングループ検出装置。

【０１９６】

（付記７）

コンピュータが、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をＩＰヘッダ中に有するパケットの個数を、計数する計数部と、

前記計数部において計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別部と、

前記判別部において前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティングループの発生の兆候がある旨を出力する出力部と
を備えることを特徴とするルーティングループ検出装置。

【０１９７】

（付記８）

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によってキャプチャされた全てのパケットの中から、時間超過メッセージ付きパケットを抽出するパケット抽出手段，

前記パケット抽出手段が抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先ＩＰアドレスを読み取る読取手段，

前記読取手段が読み取った送信先ＩＰアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信するパケット送信手段，

前記パケット送信手段が送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信するパケット受信手段，及び、

前記パケット受信手段が受信したパケットが時間超過メッセージ付きパケットであった場合に、ルーティングループが発生している旨を出力する出力手段
として機能させる
ルーティングループ検出プログラムを格納した
ことを特徴とするコンピュータ可読媒体。

【０１９８】

（付記９）

コンピュータを、

ネットワークに接続されるパケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得した場合に、取り得る全てのホップ数のそれぞれについて、そのホップ数をＩＰヘッダ中に有するパケットの個数を、計数する計数手段，

前記計数手段が計数したホップ数毎のパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別する判別手段，及び、

前記判別手段が前記ヒストグラムに平坦部又は鋸歯状部があると判別した場合にのみ、ルーティングループの発生の兆候がある旨を出力する出力手段
として機能させる
ルーティングループ検出プログラムを格納した
ことを特徴とするコンピュータ可読媒体。

【０１９９】

（付記１０）

少なくとも２台のルータを備えるネットワークにおいて、

ルータ同士を隣接させる全ての経路にそれぞれパケットキャプチャ装置を組み込んでおき、

第１のコンピュータが、

前記パケットキャプチャ装置によって所定期間キャプチャされた全てのパケットを取得

すると、取り得る全てのホップ数のそれぞれについて、そのホップ数をＩＰヘッダ中に有するパケットの個数を、計数し、

ホップ数毎に計数されたパケットの個数に基づくヒストグラムにおいて、平坦部又は鋸歯状部の有無を判別し、

前記ヒストグラムにおいて平坦部又は鋸歯状部があると判別した場合には、そのパケットキャプチャ装置においてルーティングループの発生の兆候が検出されたとして、そのパケットキャプチャ装置に対応するルータのＩＰアドレスを第２のコンピュータへ通知し、

その通知を受けた第２のコンピュータが、

前記ネットワーク中の最上流側にあるゲートウエイルータの直後に配置されているパケットキャプチャ装置において、そのゲートウエイルータから外部ネットワークへ流出するパケットがキャプチャされると、キャプチャされた全てのパケットの中から時間超過メッセージ付きパケットを抽出し、

抽出したパケットの時間超過メッセージの中から、破棄されたパケットの送信先ＩＰアドレスを読み取り、

読み取った送信先ＩＰアドレス宛へ、調査用パケットを、前記ネットワークに接続された通信装置を通じて送信し、

送信した調査用パケットについての応答として前記通信装置を通じてパケットを受信し、

受信したパケットが時間超過メッセージ付きパケットであった場合に、そのパケットの送信元のＩＰアドレスが、前記第２のコンピュータから通知されたルータのＩＰアドレスと同じであるか否かを判別し、

当該ＩＰアドレスが前記第２のコンピュータから通知されたルータのＩＰアドレスと同じであると判別した場合に、ルーティングループがそのルータにおいて発生している旨を、出力する

ことを特徴とするルーティングループ検出方法。

【図面の簡単な説明】

【０２００】

【図１】本発明が適用されたネットワークを概略的に示す構成図

【図２】第１のルーティングループ検出装置を概略的に示す構成図

【図３】第２のルーティングループ検出装置を概略的に示す構成図

【図４】第１のルーティングループ検出処理の内容を説明するためのフローチャート

【図５】集計処理の内容を説明するためのフローチャート

【図６】解析処理の内容を説明するためのフローチャート

【図７】ルーティングループが発生していない場合でのヒストグラムの一例を示す例示図

【図８】ルーティングループが発生している場合でのヒストグラムの一例を示す例示図

【図９】ルーティングループが発生している場合にヒストグラムに出現する鋸歯状部の一例を示す例示図

【図１０】第２のルーティングループ検出処理の内容を説明するためのフローチャート

【図１１】監視処理の内容を説明するためのフローチャート

【図１２】調査処理の内容を説明するためのフローチャート

【図１３】調査処理の内容を説明するためのフローチャート

【図１４】ループ位置特定処理サブルーチンの内容を説明するためのフローチャート

【図１５】本実施形態の変形例での監視処理を説明するためのフローチャート

【符号の説明】

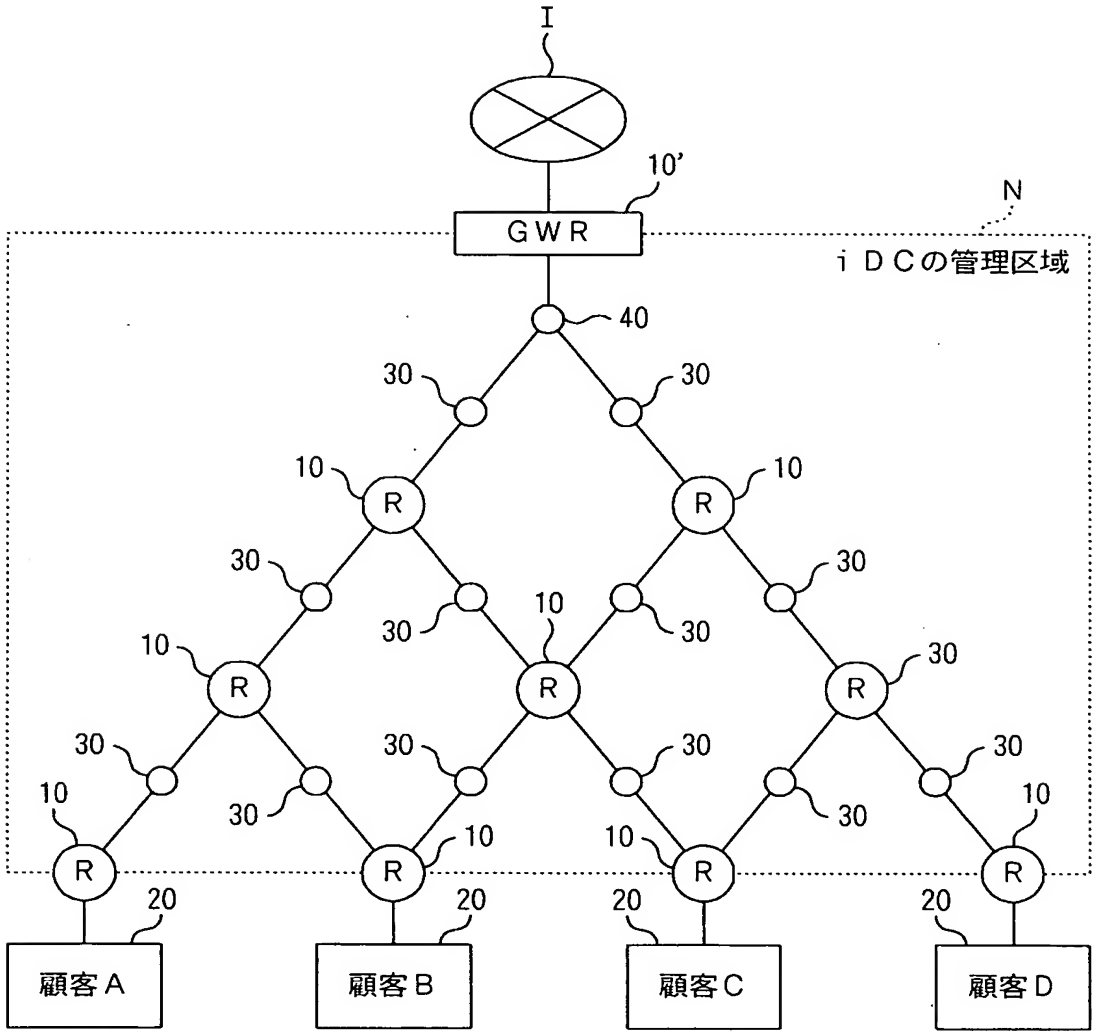
【０２０１】

１０　　ルータ

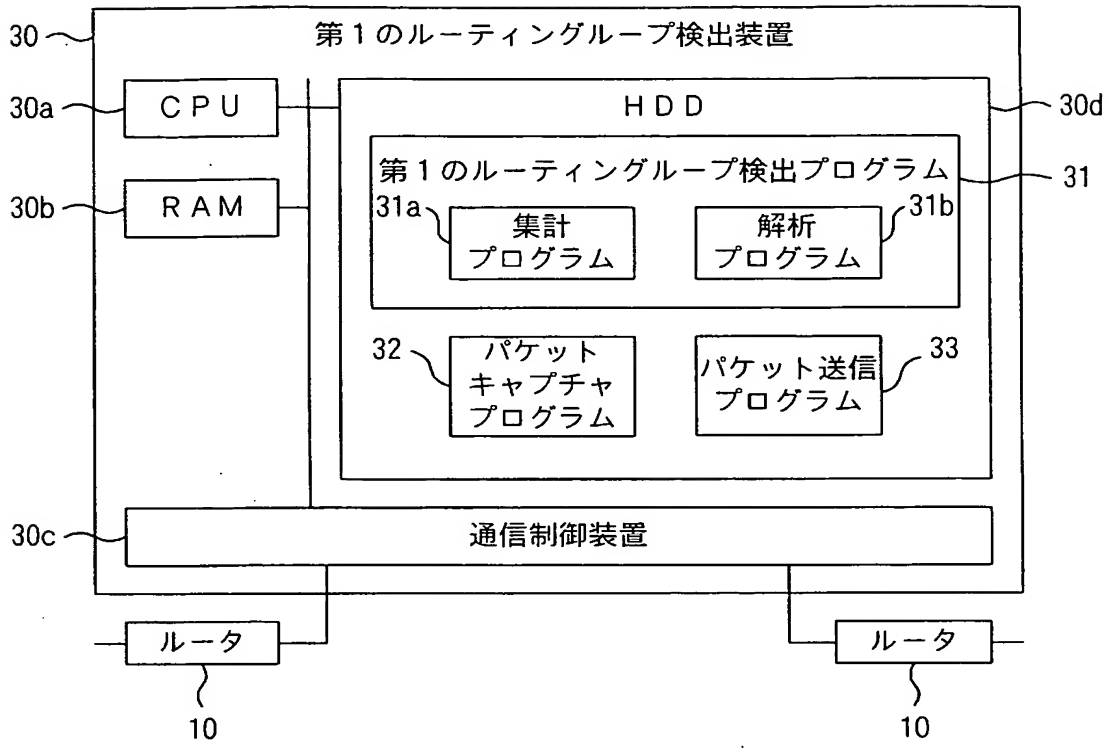
１０’　ゲートウエイルータ

３０　第１のルーティングループ検出装置
３０ａ　ＣＰＵ
３０ｂ　ＲＡＭ
３０ｃ　通信制御装置
３０ｄ　ＨＤＤ
３１　第１のルーティングループ検出プログラム
３２　パケットキャプチャプログラム
３３　パケット送信プログラム
４０　第２のルーティングループ検出装置
４０ａ　ＣＰＵ
４０ｂ　ＲＡＭ
４０ｃ　通信制御装置
４０ｄ　ＨＤＤ
４１　第２のルーティングループ検出プログラム
４２　パケットキャプチャプログラム
４３　パケット受信プログラム

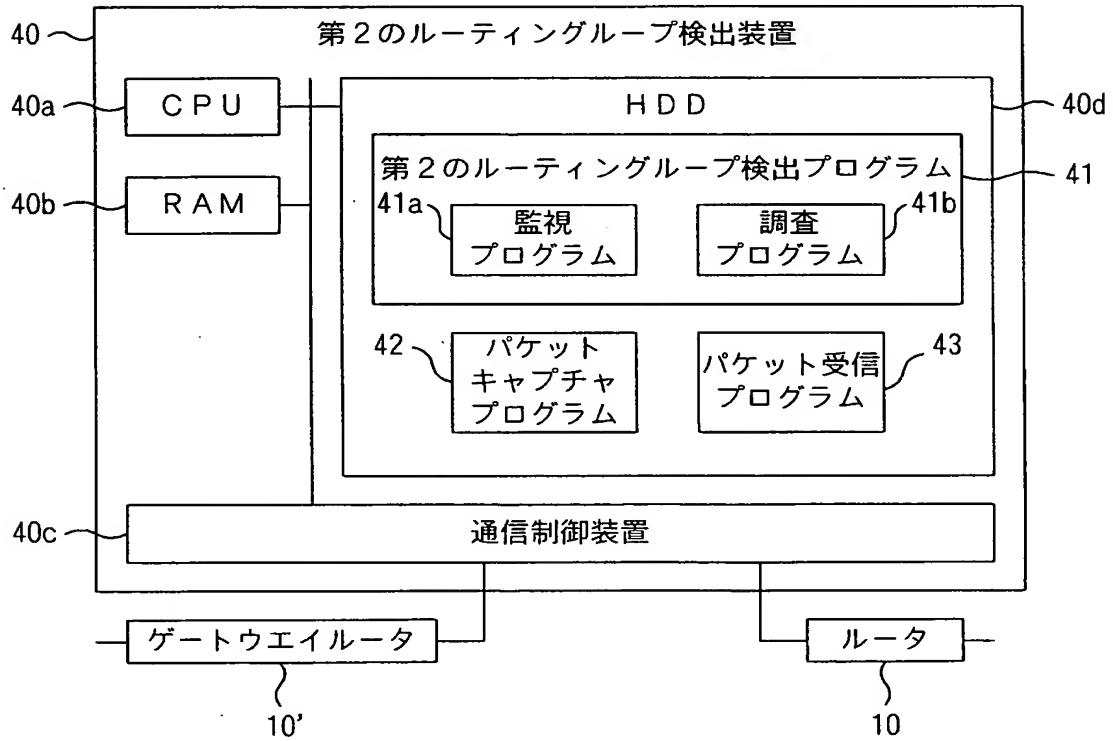
【書類名】図面
【図１】



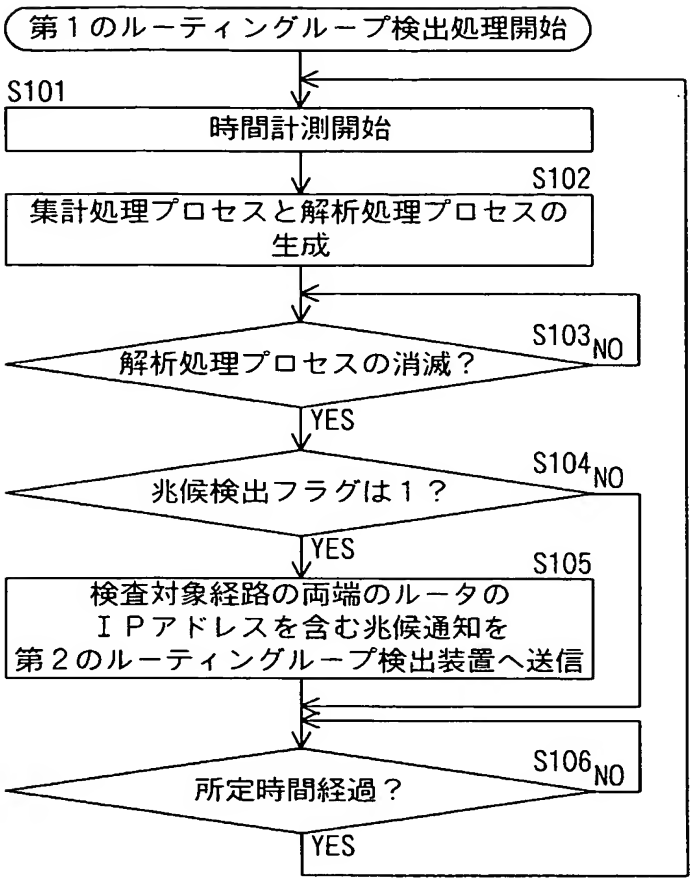
【図２】


30
第１のルーティングループ検出装置
30a
ＣＰＵ
30b
ＲＡＭ
ＨＤＤ
30d
第１のルーティングループ検出プログラム
31
31a
集計
プログラム
解析
プログラム
31b
32
パケット
キャプチャ
プログラム
パケット送信
プログラム
33
30c
通信制御装置
ルータ
ルータ
10
10

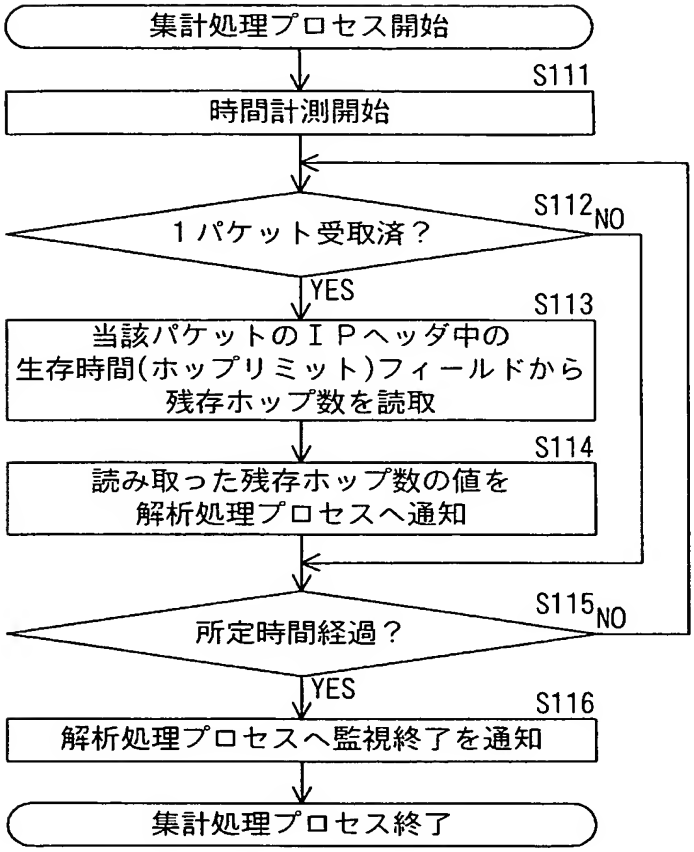
【図３】


40
第２のルーティングループ検出装置
40a
ＣＰＵ
40b
ＲＡＭ
ＨＤＤ
40d
第２のルーティングループ検出プログラム
41
41a
監視
プログラム
調査
プログラム
41b
42
パケット
キャプチャ
プログラム
パケット受信
プログラム
43
40c
通信制御装置
ゲートウエイルータ
ルータ
10'
10

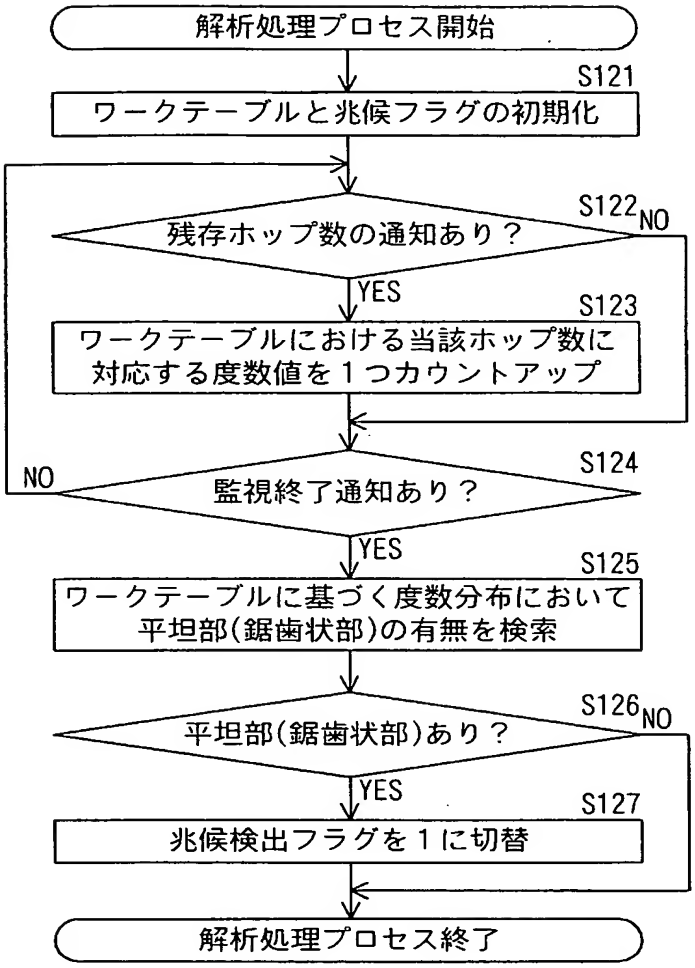
【図４】


第１のルーティングループ検出処理開始
S101
時間計測開始
S102
集計処理プロセスと解析処理プロセスの生成
S103
NO
解析処理プロセスの消滅？
YES
S104
NO
兆候検出フラグは１？
YES
S105
検査対象経路の両端のルータのＩＰアドレスを含む兆候通知を第２のルーティングループ検出装置へ送信
S106
NO
所定時間経過？
YES

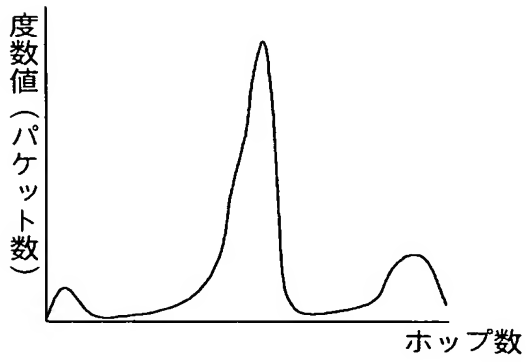
【図５】


集計処理プロセス開始
S111
時間計測開始
S112
NO
１パケット受取済？
YES
S113
当該パケットのＩＰヘッダ中の
生存時間(ホップリミット)フィールドから
残存ホップ数を読取
S114
読み取った残存ホップ数の値を
解析処理プロセスへ通知
S115
NO
所定時間経過？
YES
S116
解析処理プロセスへ監視終了を通知
集計処理プロセス終了

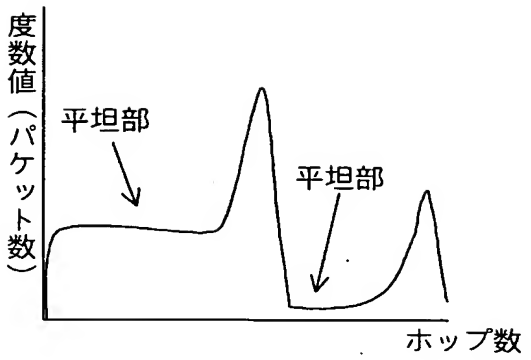
【図６】


解析処理プロセス開始
S121
ワークテーブルと兆候フラグの初期化
S122
残存ホップ数の通知あり？
NO
YES
S123
ワークテーブルにおける当該ホップ数に
対応する度数値を１つカウントアップ
S124
NO
監視終了通知あり？
YES
S125
ワークテーブルに基づく度数分布において
平坦部(鋸歯状部)の有無を検索
S126
平坦部(鋸歯状部)あり？
NO
YES
S127
兆候検出フラグを１に切替
解析処理プロセス終了

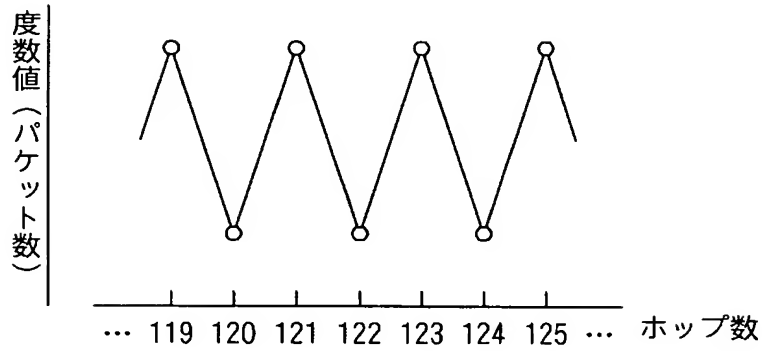
【図７】


度数値（パケット数）
ホップ数

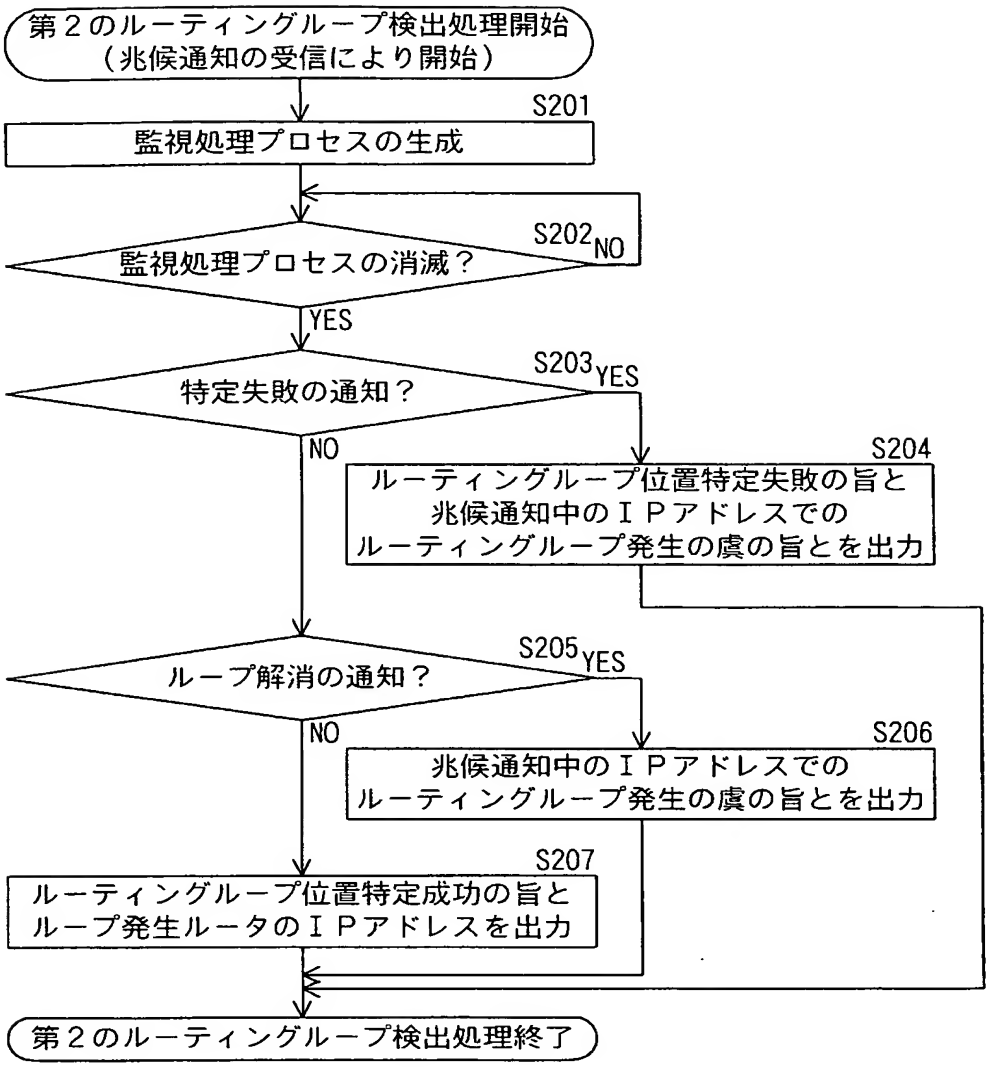
【図８】


度数値（パケット数）
平坦部
平坦部
ホップ数

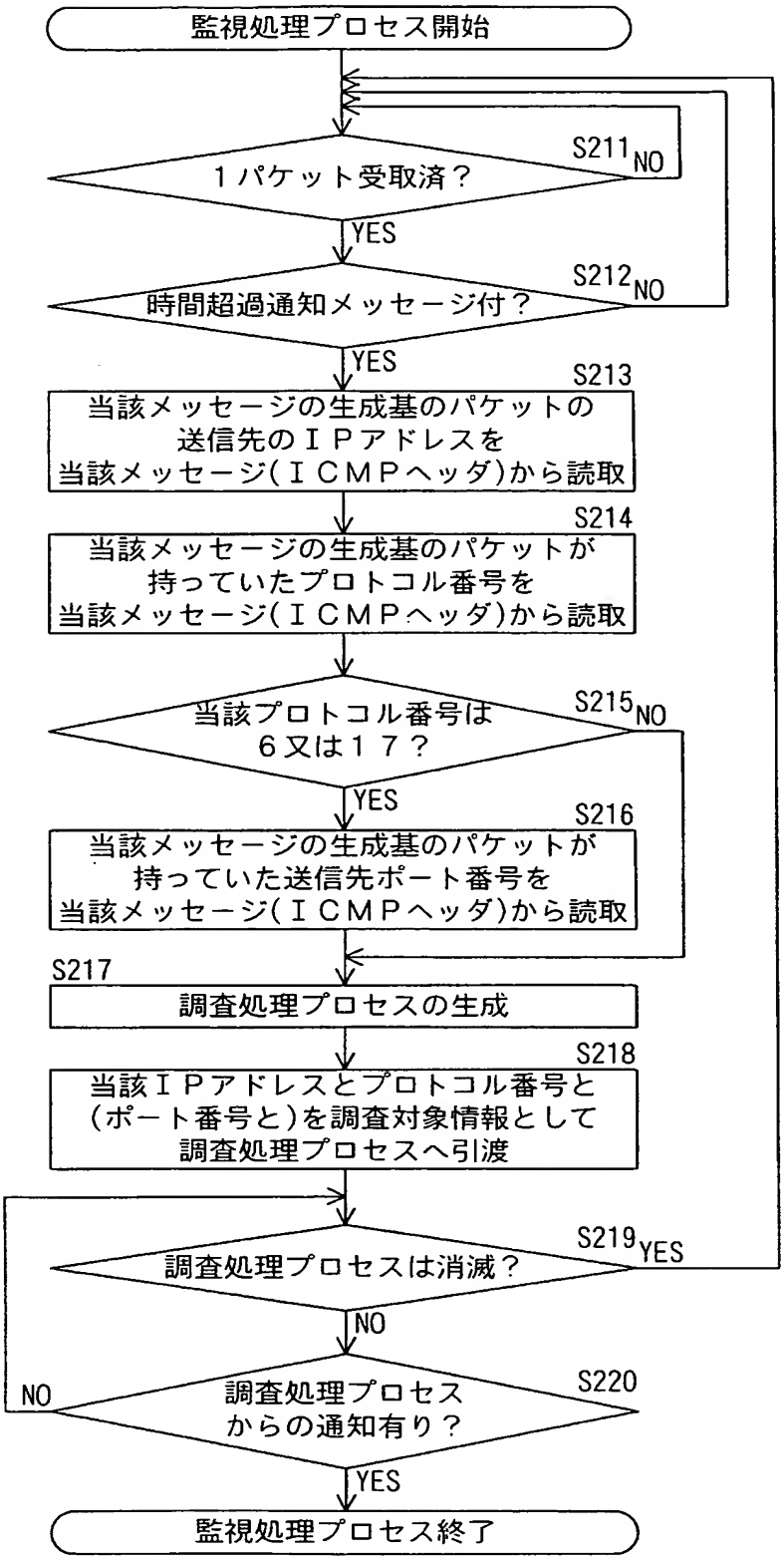
【図９】


度数値（パケット数）
… 119 120 121 122 123 124 125 …
ホップ数

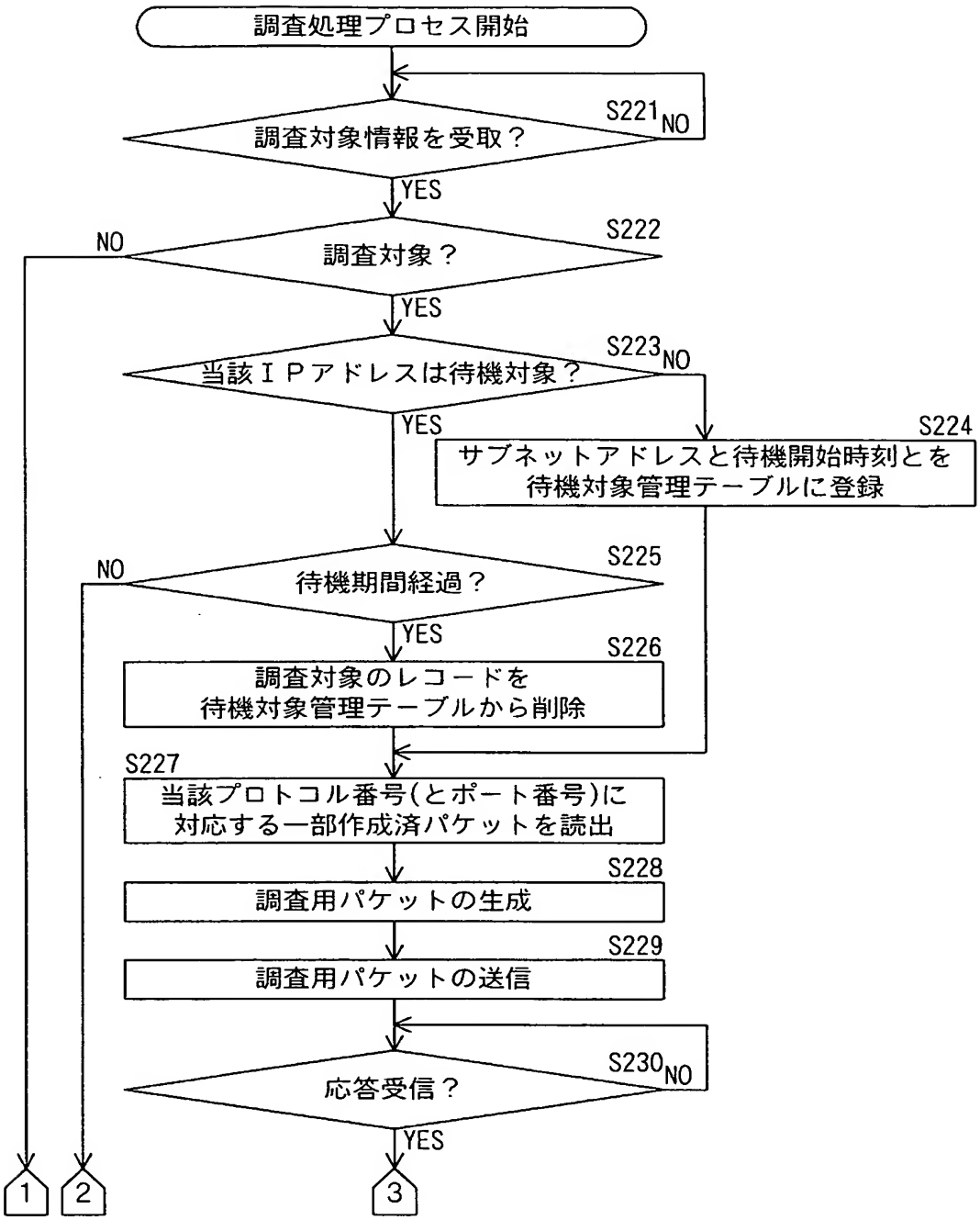
【図１０】


第２のルーティングループ検出処理開始
（兆候通知の受信により開始）
S201
監視処理プロセスの生成
S202
NO
監視処理プロセスの消滅？
YES
S203
YES
特定失敗の通知？
NO
S204
ルーティングループ位置特定失敗の旨と
兆候通知中のＩＰアドレスでの
ルーティングループ発生の虞の旨とを出力
S205
YES
ループ解消の通知？
NO
S206
兆候通知中のＩＰアドレスでの
ルーティングループ発生の虞の旨とを出力
S207
ルーティングループ位置特定成功の旨と
ループ発生ルータのＩＰアドレスを出力
第２のルーティングループ検出処理終了

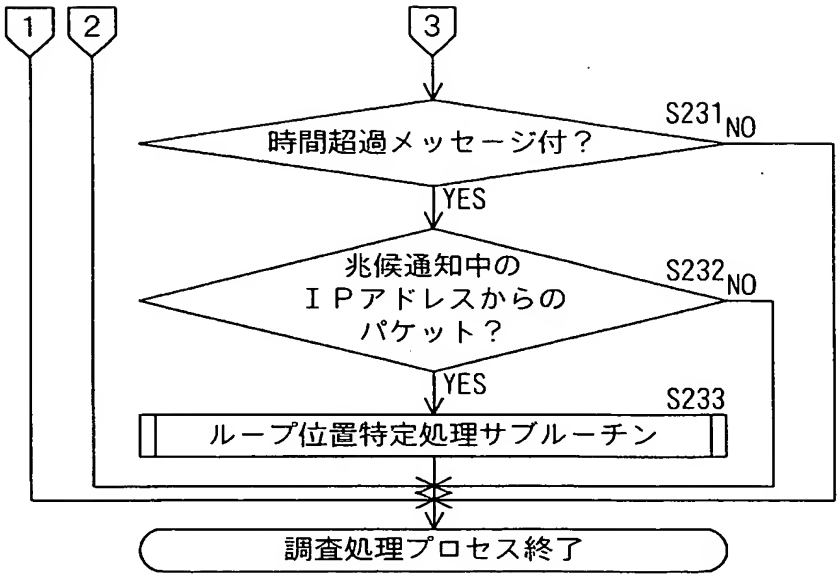
【図１１】


監視処理プロセス開始
S211
１パケット受取済？
NO
YES
S212
時間超過通知メッセージ付？
NO
YES
S213
当該メッセージの生成基のパケットの
送信先のＩＰアドレスを
当該メッセージ(ＩＣＭＰヘッダ)から読取
S214
当該メッセージの生成基のパケットが
持っていたプロトコル番号を
当該メッセージ(ＩＣＭＰヘッダ)から読取
S215
当該プロトコル番号は
６又は１７？
NO
YES
S216
当該メッセージの生成基のパケットが
持っていた送信先ポート番号を
当該メッセージ(ＩＣＭＰヘッダ)から読取
S217
調査処理プロセスの生成
S218
当該ＩＰアドレスとプロトコル番号と
(ポート番号と)を調査対象情報として
調査処理プロセスへ引渡
S219
調査処理プロセスは消滅？
YES
NO
S220
調査処理プロセス
からの通知有り？
NO
YES
監視処理プロセス終了

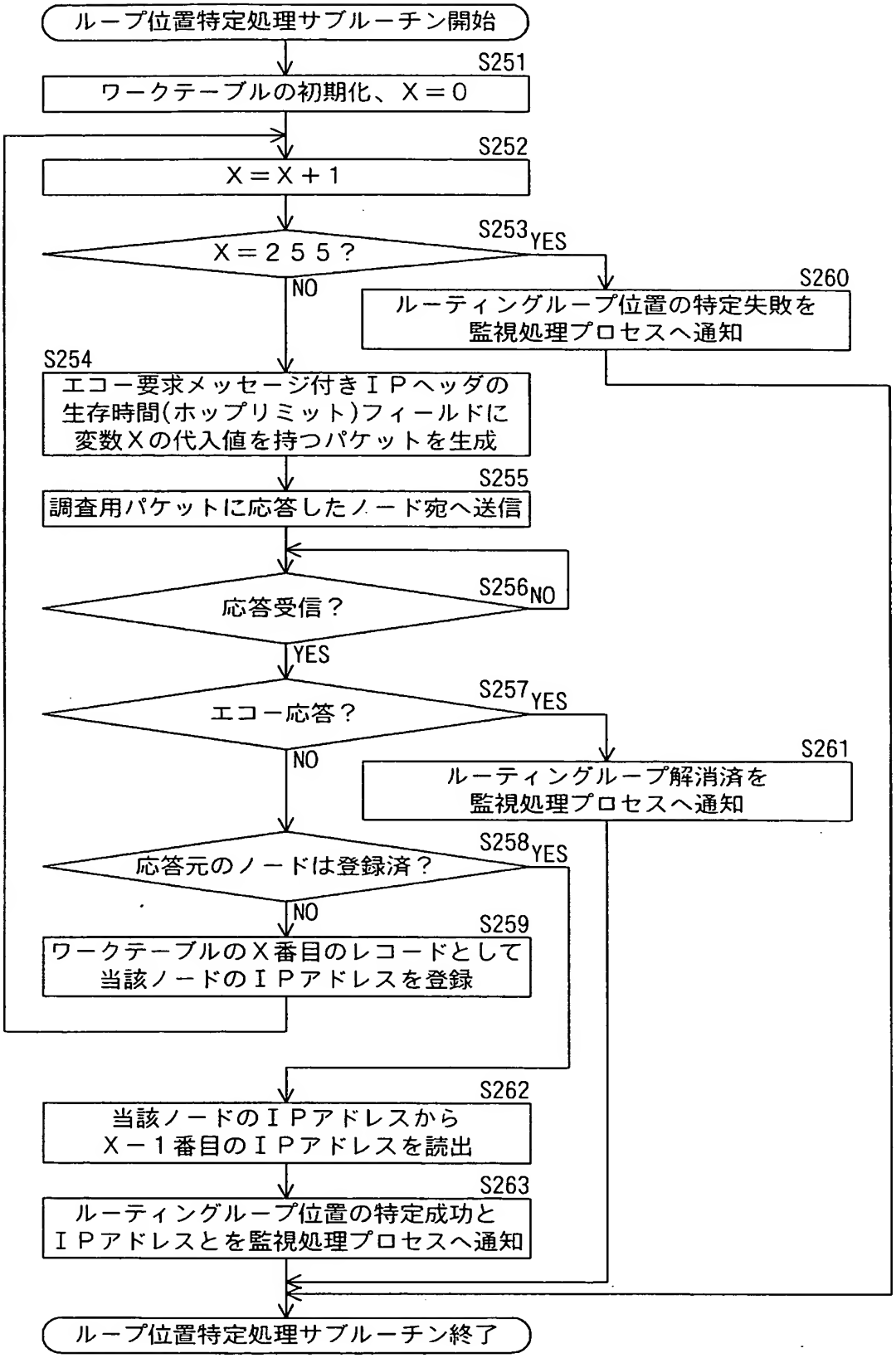
【図１２】


調査処理プロセス開始
S221
調査対象情報を受取？
NO
YES
S222
調査対象？
NO
YES
S223
当該ＩＰアドレスは待機対象？
NO
YES
S224
サブネットアドレスと待機開始時刻とを
待機対象管理テーブルに登録
S225
待機期間経過？
NO
YES
S226
調査対象のレコードを
待機対象管理テーブルから削除
S227
当該プロトコル番号(とポート番号)に
対応する一部作成済パケットを読出
S228
調査用パケットの生成
S229
調査用パケットの送信
S230
応答受信？
NO
YES
1
2
3

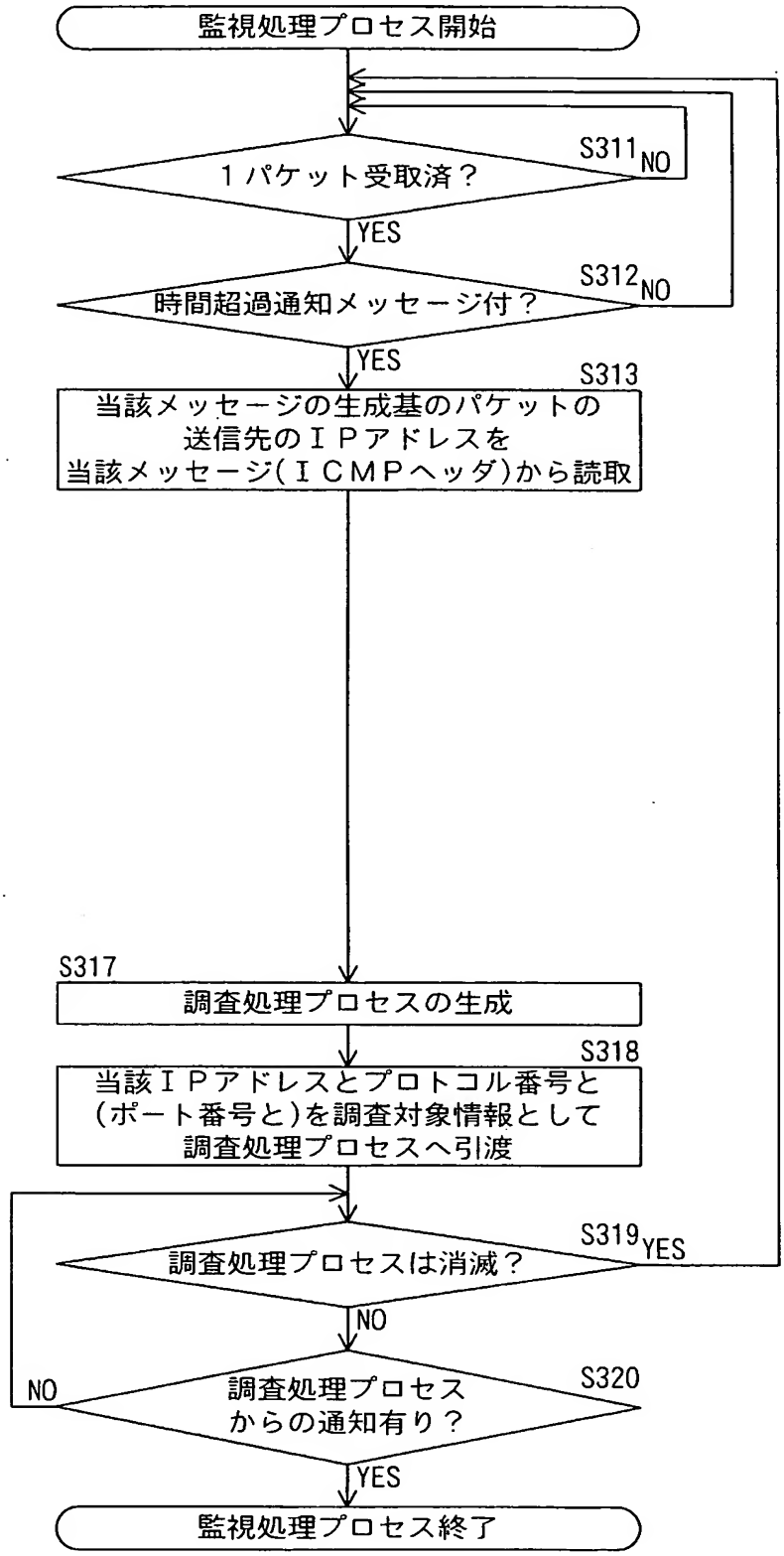
【図１３】


1
2
3
時間超過メッセージ付？
S231
NO
YES
兆候通知中の
ＩＰアドレスからの
パケット？
S232
NO
YES
S233
ループ位置特定処理サブルーチン
調査処理プロセス終了

【図１４】


ループ位置特定処理サブルーチン開始
S251
ワークテーブルの初期化、Ｘ＝０
S252
Ｘ＝Ｘ＋１
S253
Ｘ＝２５５？
YES
NO
S260
ルーティングループ位置の特定失敗を
監視処理プロセスへ通知
S254
エコー要求メッセージ付きＩＰヘッダの
生存時間(ホップリミット)フィールドに
変数Ｘの代入値を持つパケットを生成
S255
調査用パケットに応答したノード宛へ送信
S256
応答受信？
NO
YES
S257
エコー応答？
YES
NO
S261
ルーティングループ解消済を
監視処理プロセスへ通知
S258
応答元のノードは登録済？
YES
NO
S259
ワークテーブルのＸ番目のレコードとして
当該ノードのＩＰアドレスを登録
S262
当該ノードのＩＰアドレスから
Ｘ－１番目のＩＰアドレスを読出
S263
ルーティングループ位置の特定成功と
ＩＰアドレスとを監視処理プロセスへ通知
ループ位置特定処理サブルーチン終了

【図１５】


監視処理プロセス開始
S311
１パケット受取済？
NO
YES
S312
時間超過通知メッセージ付？
NO
YES
S313
当該メッセージの生成基のパケットの
送信先のＩＰアドレスを
当該メッセージ(ＩＣＭＰヘッダ)から読取
S317
調査処理プロセスの生成
S318
当該ＩＰアドレスとプロトコル番号と
(ポート番号と)を調査対象情報として
調査処理プロセスへ引渡
S319
調査処理プロセスは消滅？
YES
NO
S320
調査処理プロセス
からの通知有り？
NO
YES
監視処理プロセス終了

【書類名】要約書
【要約】
【課題】ネットワークの規模に拘わらずルーティングループを確実且つ即時に検出するためのルーティングループ検出プログラム及びルーティングループ検出方法を、提供する。
【解決手段】第１ルーティングループ検出装置３０は、ネットワークＮにおけるルータ１０同士を隣接させる全ての経路を下流に向かって流れるパケットを所定期間キャプチャし、ホップ数毎にパケットの個数を計数することによってヒストグラムを生成し、ヒストグラムにおける平坦部分の有無を判別することにより、ルーティングループの発生の兆候を検出する。第２のルーティングループ検出装置４０は、ゲートウエイルータ１０’の下流側においてそのゲートウエイルータ１０’から外部へ流出する時間超過メッセージ付きパケットをキャプチャし、元の送信先へ調査用パケットを送信し、その応答として時間超過メッセージ付きパケットを受信することにより、ルーティングループの発生を検出する。
【選択図】図１

特願２００３－３２６１７３

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社